Billing code 4410-09-P

DEPARTMENT OF JUSTICE

Drug Enforcement Administration

21 CFR Parts 1300, 1304, 1306, 1311

[Docket No. DEA-218I]

RIN 1117-AA61

Electronic Prescriptions for Controlled Substances

AGENCY: Drug Enforcement Administration (DEA), Department of Justice

ACTION: Interim Final Rule with Request for Comment.

SUMMARY: The Drug Enforcement Administration (DEA) is revising its regulations to provide practitioners with the option of writing prescriptions for controlled substances electronically. The regulations will also permit pharmacies to receive, dispense, and archive these electronic prescriptions. These regulations are an addition to, not a replacement of, the existing rules. The regulations provide pharmacies, hospitals, and practitioners with the ability to use modern technology for controlled substance prescriptions while maintaining the closed system of controls on controlled substances dispensing; additionally, the regulations will reduce paperwork for DEA registrants who dispense controlled substances and have the potential to reduce prescription forgery. The regulations will also have the potential to reduce the number of prescription errors caused by illegible handwriting and misunderstood oral prescriptions. Moreover, they will help both pharmacies and hospitals to integrate prescription records into other medical records

more directly, which may increase efficiency, and potentially reduce the amount of time patients spend waiting to have their prescriptions filled.

DATES: This rule has been classified as a major rule subject to Congressional review. The effective date is [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]. However, at the conclusion of the Congressional review, if the effective date has been changed, the Drug Enforcement Administration will publish a document in the Federal Register to establish the actual effective date or to terminate the rule.

The incorporation by reference of certain publications listed in the rule is approved by the Director of the Federal Register as of [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

Written comments must be postmarked and electronic comments must be submitted on or before [INSERT DATE 60 DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER]. Commenters should be aware that the electronic Federal Docket Management System will not accept comments after Midnight Eastern Time on the last day of the comment period.

ADDRESSES: To ensure proper handling of comments, please reference "Docket No. DEA-218" on all written and electronic correspondence. Written comments sent via regular or express mail should be sent to the Drug Enforcement Administration, Attention: DEA Federal Register Representative/ODL, 8701 Morrissette Drive, Springfield, VA 22152. Comments may be sent to DEA by sending an electronic message to dea.diversion.policy@usdoj.gov. Comments may also be sent electronically through http://www.regulations.gov using the electronic comment form provided on that

site. An electronic copy of this document is also available at the http://www.regulations.gov web site. DEA will accept attachments to electronic comments in Microsoft word, WordPerfect, Adobe PDF, or Excel file formats only. DEA will not accept any file formats other than those specifically listed here.

Please note that DEA is requesting that electronic comments be submitted before midnight Eastern Time on the day the comment period closes because http://www.regulations.gov terminates the public's ability to submit comments at midnight Eastern Time on the day the comment period closes. Commenters in time zones other than Eastern Time may want to consider this so that their electronic comments are received. All comments sent via regular or express mail will be considered timely if postmarked on the day the comment period closes.

FOR FURTHER INFORMATION CONTACT: Mark W. Caverly, Chief, Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152, Telephone (202) 307-7297.

SUPPLEMENTARY INFORMATION

Comments: DEA is seeking additional comments on the following issues: identity proofing, access control, authentication, biometric subsystems and testing of those subsystems, internal audit trails for electronic prescription applications, and third-party auditors and certification organizations.

POSTING OF PUBLIC COMMENTS: Please note that all comments received are considered part of the public record and made available for public inspection online at http://www.regulations.gov and in the Drug Enforcement Administration's public docket.

Such information includes personal identifying information (such as your name, address, etc.) voluntarily submitted by the commenter.

If you want to submit personal identifying information (such as your name, address, etc.) as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase "PERSONAL IDENTIFYING INFORMATION" in the first paragraph of your comment. You must also place all the personal identifying information you do not want posted online or made available in the public docket in the first paragraph of your comment and identify what information you want redacted.

If you want to submit confidential business information as part of your comment, but do not want it to be posted online or made available in the public docket, you must include the phrase "CONFIDENTIAL BUSINESS INFORMATION" in the first paragraph of your comment. You must also prominently identify confidential business information to be redacted within the comment. If a comment has so much confidential business information that it cannot be effectively redacted, all or part of that comment may not be posted online or made available in the public docket.

Personal identifying information and confidential business information identified and located as set forth above will be redacted and the comment, in redacted form, will be posted online and placed in the Drug Enforcement Administration’s public docket file. Please note that the Freedom of Information Act applies to all comments received. If you wish to inspect the agency's public docket file in person by appointment, please see the "FOR FURTHER INFORMATION" paragraph.

G. Executive Order 13132
H. Unfunded Mandates Reform Act of 1995

I. Legal Authority

DEA implements the Comprehensive Drug Abuse Prevention and Control Act of 1970, often referred to as the Controlled Substances Act (CSA) and the Controlled Substances Import and Export Act (21 U.S.C. 801-971), as amended. DEA publishes the implementing regulations for these statutes in Title 21 of the Code of Federal Regulations (CFR), Parts 1300 to 1399. These regulations are designed to ensure an adequate supply of controlled substances for legitimate medical, scientific, research, and industrial purposes, and to deter the diversion of controlled substances to illegal purposes. The CSA mandates that DEA establish a closed system of control for manufacturing, distributing, and dispensing controlled substances. Any person who manufactures, distributes, dispenses, imports, exports, or conducts research or chemical analysis with controlled substances must register with DEA (unless exempt) and comply with the applicable requirements for the activity.

Controlled Substances

Controlled substances are drugs and other substances that have a potential for abuse and psychological and physical dependence; these include opioids, stimulants, depressants, hallucinogens, anabolic steroids, and drugs that are immediate precursors of these classes of substances. DEA lists controlled substances in 21 CFR part 1308. The substances are divided into five schedules: Schedule I substances have a high potential for abuse and have no currently accepted medical use in treatment in the United States. These substances may only be used for research, chemical analysis, or manufacture of other drugs. Schedule II – V substances have currently accepted medical uses in the

United States, but also have potential for abuse and psychological and physical dependence that necessitate control of the substances under the CSA. The vast majority of Schedule II, III, IV, and V controlled substances are available only pursuant to a prescription issued by a practitioner licensed by the State and registered with DEA to dispense the substances. Overall, controlled substances constitute between 10 percent and 11 percent of all prescriptions written in the United States.

II. Regulatory History

The Controlled Substances Act and Current Regulations. The CSA and DEA's regulations were originally adopted at a time when most transactions and particularly prescriptions were done on paper.

The CSA provides that a controlled substance in Schedule II may only be dispensed by a pharmacy pursuant to a "written prescription," except in emergency situations (21 U.S.C. 829(a)). In contrast, for controlled substances in Schedules III and IV, the CSA provides that a pharmacy may dispense pursuant to a "written or oral prescription." (21 U.S.C. 829(b)). Where an oral prescription is permitted by the CSA, the DEA regulations further provide that a practitioner may transmit to the pharmacy a facsimile of a written, manually signed prescription in lieu of an oral prescription (21 CFR 1306.21(a)).

Under longstanding Federal law, for a prescription for a controlled substance to be valid, it must be issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice (United States v. Moore, 423 U.S. 122 (1975); 21 CFR 1306.04(a)). As the DEA regulations state: "The responsibility for the proper prescribing and dispensing of controlled substances is upon the prescribing practitioner,

but a corresponding responsibility rests with the pharmacist who fills the prescription." (21 CFR 1306.04(a)).

The Controlled Substances Act is unique among criminal laws in that it stipulates acts pertaining to controlled substances that are permissible. That is, if the CSA does not explicitly permit an action pertaining to a controlled substance, then by its lack of explicit permissibility the act is prohibited. Violations of the Act can be civil or criminal in nature, which may result in administrative, civil, or criminal proceedings. Remedies under the Act can range from modification or revocation of DEA registration, to civil monetary penalties or imprisonment, depending on the nature, scope, and extent of the violation.

Specifically, it is unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, a controlled substance or to possess a controlled substance with the intent of manufacturing, distributing, or dispensing that controlled substance, except as authorized by the Controlled Substances Act (21 U.S.C. 841(a)(1)).

Further, it is unlawful for any person knowingly or intentionally to possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, issued for a legitimate medical purpose, from a practitioner, while acting in the course of the practitioner's professional practice, or except as otherwise authorized by the CSA (21 U.S.C. 844(a)). It is unlawful for any person to knowingly or intentionally acquire or obtain possession of a controlled substance by misrepresentation, fraud, forgery, deception, or subterfuge (21 U.S.C. 843(a)(3)).

It is unlawful for any person knowingly or intentionally to use a DEA registration number that is fictitious, revoked, suspended, expired, or issued to another person in the

course of dispensing a controlled substance, or for the purpose of acquiring or obtaining a controlled substance (21 U.S.C. 843(a)(2)).

Beyond these possession and dispensing requirements, it is unlawful for any person to refuse or negligently fail to make, keep, or furnish any record (including any record of dispensing) that is required by the CSA (21 U.S.C. 842(a)(5)). It is also unlawful to furnish any false or fraudulent material information in, or omit any information from, any record required to be made or kept (21 U.S.C. 843(a)(4)(A)).

Within the CSA's system of controls, it is the individual practitioner (e.g., physician, dentist, veterinarian, nurse practitioner) who issues the prescription authorizing the dispensing of the controlled substance. This prescription must be issued for a legitimate medical purpose and must be issued in the usual course of professional practice. The individual practitioner is responsible for ensuring that the prescription conforms to all legal requirements. The pharmacist, acting under the authority of the DEA-registered pharmacy, has a corresponding responsibility to ensure that the prescription is valid and meets all legal requirements. The DEA-registered pharmacy does not order the dispensing. Rather, the pharmacy, and the dispensing pharmacist merely rely on the prescription as written by the DEA-registered individual practitioner to conduct the dispensing.

Thus, a prescription is much more than the mere method of transmitting dispensing information from a practitioner to a pharmacy. The prescription serves both as a record of the practitioner's determination of the legitimate medical need for the drug to be dispensed, and as a record of the dispensing, providing the pharmacy with the legal justification and authority to dispense the medication prescribed by the practitioner. The

prescription also provides a record of the actual dispensing of the controlled substance to the ultimate user (the patient) and, therefore, is critical to documenting that controlled substances held by a pharmacy have been dispensed legally. The maintenance by pharmacies of complete and accurate prescription records is an essential part of the overall CSA regulatory scheme established by Congress.

American Recovery and Reinvestment Act. On February 17, 2009, the President signed the American Recovery and Reinvestment Act of 2009 (Recovery Act) (Pub. L. 111-5, 123 STAT. 115). Among its many provisions, the Recovery Act promotes the "meaningful use" of electronic health records (EHRs) via incentives. The health information technology provisions of the Recovery Act are primarily found in Title XIII, Division A, Health Information Technology, and in Title IV of Division B, Medicare and Medicaid Health Information Technology. These titles together are cited as the Health Information Technology for Economic and Clinical Health Act or the HITECH Act. Under Title IV, the Medicare and Medicaid health information technology provisions in the Recovery Act provide incentives and support for the adoption of certified electronic health record technology. The Recovery Act authorizes incentive payments for eligible professionals and eligible hospitals participating in Medicare or Medicaid if they can demonstrate to the Secretary of HHS that they are “meaningful EHR users” as defined by the Act and its implementing regulations. Such incentive payments to encourage electronic prescribing are allowed, but penalties in any form, by third party payers are prohibited. These incentive payments will begin in 2011.

On January 13, 2010, HHS published two rules to implement the provisions of the HITECH ACT. The Centers for Medicare and Medicaid Services published a notice of

proposed rulemaking entitled “Medicare and Medicaid Programs; Electronic Health Record Incentive Program” (75 FR 1844) [CMS-0033-P, RIN 0938-AP78]. The proposed rule would specify the initial criteria an eligible professional and eligible hospital must meet to qualify for the incentive payment; calculation of the incentive payment amounts; and other payment and program participation issues.

The Office of the National Coordinator for Health Information Technology published an interim final rule entitled “Health Information Technology; Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology” (75 FR 2014) [RIN 0991-AB58]. The interim final rule became effective February 12, 2010. The certification criteria adopted in the interim final rule establish the capabilities and related standards that certified electronic health record technology will need to include in order to, at a minimum, support the achievement of the proposed meaningful use Stage 1 (beginning in 2011) by eligible professionals and eligible hospitals under the Medicare and Medicaid EHR incentive programs. The comment period for both rules ended March 15, 2010.

The Office of the National Coordinator for Health Information Technology also published a notice of proposed rulemaking entitled “Proposed Establishment of Certification Programs for Health Information Technology” (75 FR 11328, March 10, 2010) (RIN 0991-AB59) which proposes the establishment of certification programs for purposes of testing and certifying health information technology. The proposed rule specifies the processes the National Coordinator for Health Information Technology would follow to authorize organizations to perform the certification of health information technology.

Electronic Prescription Applications. Electronic prescription applications[1] and electronic health record (EHR) applications have been available for a number of years and are anticipated by many to improve healthcare and possibly reduce costs by increasing compliance with formularies and the use of generic medications. Electronic prescriptions may reduce medical errors caused by illegible handwriting. Adoption of these applications has been relatively slow, primarily because of their cost, the disruption caused during implementation, and lack of mature standards that allow for interoperability among applications.[2] Some have also expressed a concern about the inability to use electronic prescription applications for all prescriptions.

Electronic prescription applications may be stand-alone applications (i.e., applications that only create prescriptions) or they may be integrated into EHR applications that create and link all medical records and associated information.[3] Either type of application may be installed on a practitioner's computers (installed applications) or may be an Internet-based application, where the practitioner accesses the application through the Internet; for these latter applications, the application service provider (ASP) retains the records on its servers. For most practitioners and pharmacies, the applications are purchased from application providers. Some large healthcare systems and chain

[1] "Application" means a software program used to perform a set of functions.
[2] California Healthcare Foundation. "Gauging the Progress of the National Health IT Technology Initiative", January 2008; Congressional Budget Office, Evidence on the Costs and Benefits of Health IT, May 2008.
[3] The National Alliance for Health Information Technology has defined the terms "electronic Medical record (EMR)," "electronic health record (EHR)," and "personal health record (PHR." Both EMRs and EHRs are defined to be maintained by practitioners, whereas a PHR is defined to be maintained by the individual patient. The main distinction between an EMR and an EHR is the EHR's ability to exchange information interoperably. DEA's use of the term EHR in this rule relates to those records maintained by practitioners, as opposed to a PHR maintained by an individual patient, regardless of how those records are maintained.

pharmacies, however, may develop and maintain the applications themselves, serving as both the practitioner or pharmacy and the application provider.

The existing electronic prescription applications allow practitioners to create a prescription electronically, but accommodate different means of transmitting the prescription to the pharmacy. Practitioners may print the prescription for manual signature; the prescription may then be given to the patient or the practitioner's office may fax it to a pharmacy. Some applications will automatically transmit an image of the prescription as a facsimile. True electronic prescriptions, however, are transmitted as electronic data files to the pharmacy, whose applications import the data file into its database. Virtually all pharmacies maintain prescription records electronically; prescriptions that are not received as electronic data files are manually entered into the pharmacy application.

Because of the large number of electronic prescription and pharmacy applications and the current lack of a mature standard for the formatting of prescription data, most electronic prescriptions are routed from the electronic prescription or EHR application through intermediaries, at least one of which determines whether the prescription file needs to be converted from one software version to another so that the receiving pharmacy application can correctly import the data. There are generally three to five intermediaries that route prescriptions between practitioners and pharmacies. For example, a prescription may be routed to the application provider, then to a hub that converts the prescription from one software version to another to meet the requirements of the receiving pharmacy, then to the pharmacy application provider or chain pharmacy server before reaching the dispensing pharmacy. Some application providers further

route prescriptions through aggregators who direct the prescription to a hub or to a pharmacy. For closed healthcare systems, where the practitioners and pharmacies are part of the same system, intermediaries are not needed.

Standards. Any electronic data transfer depends on the ability of the receiving application to open and read the information accurately. To be able to do this, the fields and transactions need to be defined and tagged so that the receiving application knows, for example, that a particular set of characters is a date and that other sets are names, etc. The National Council for Prescription Drug Programs (NCPDP) has developed a standard for prescriptions, called SCRIPT, which is generally used by application providers; hospital-based applications may also use Health Level 7 (HL7) standards. SCRIPT is a data transmission standard "intended to facilitate the communication of prescription information between prescribers, pharmacies, and payers."[4] It defines transactions (e.g., new prescription, refill request, prescription change, cancellation,), segments (e.g., provider, patient), and data fields within segments (e.g., name, date, quantity). Each data field has a number and a defined format (e.g., DEA number is nine characters). The standardization allows the receiving pharmacy to identify and separate the data it receives and import the information into the correct fields in the pharmacy database. SCRIPT does not address other aspects of prescription or pharmacy applications (e.g., what information is displayed and stored at a practice or pharmacy, logical access controls, audit trails). SCRIPT provides for, but does not mandate the use of, some fields (e.g., practitioner first name and patient address) that DEA requires. In addition, although the standard mandates that applications include certain fields, it does not require that those

[4] National Council for Prescription Drug Programs, Prescriber/Pharmacist Interface SCRIPT Standard Implementation Guide Version 10.0, October 2006.

fields be completed before transmission is allowed. The SCRIPT standard is still evolving; the most recent is Version 10 Release 6. The interoperability issues that require intermediaries generally relate to pharmacy and practitioner applications using different versions of the standard as well as varying approaches to providing opening and reading instructions.

One intermediary, SureScripts/RxHub, certifies electronic prescription and pharmacy applications for compliance with the SCRIPT standard; SureScripts/RxHub determines whether the electronic prescription application creates a prescription that conforms to the SCRIPT standard and whether the pharmacy application is able to open and read a SCRIPT prescription correctly.[5] SureScripts/RxHub certification does not address aspects of applications unrelated to their ability to produce or read a prescription in appropriate SCRIPT format.

The Certification Commission for Healthcare Information Technology (CCHIT) is a private, nonprofit organization recognized by the Secretary of HHS as a certification body for EHRs under the exception to the physician self-referral prohibition and safe harbor under the anti-kickback statute, respectively, for certain arrangements involving the donation of interoperable EHR software to physicians and other health care practitioners or entities (71 FR 45140 and 71 FR 45110, respectively, August 8, 2006). . CCHIT develops criteria for electronic medical records (EMRs or EHRs) and certifies applications against these criteria. Although electronic prescribing is addressed in the CCHIT ambulatory certification criteria, these criteria do not address all elements with which DEA has concern, such as the particular information required in a prescription.

[5] http://www.surescripts.com/certification.html, accessed April 29, 2009.

The CCHIT criteria do address security issues, such as access control and audit logs. CCHIT is developing standards for stand-alone electronic prescription applications. DEA has not been able to identify any organization that sets standards for or certifies pharmacy applications for security issues or even for the ability to record and retain information such as dispensing data.

Proposed Rule. On June 27, 2008, DEA published a Notice of Proposed Rulemaking (NPRM) to revise its regulations to allow the creation, signature, transmission, and processing of controlled substance prescriptions electronically (73 FR 36722). The proposed rule followed consultations with the industry and the Department of Health and Human Services, which is responsible for establishing transmission standards for electronic prescriptions and security standards for health information. The proposed rule provided two approaches, one for the private sector and one for Federal healthcare providers. The private sector approach included identity proofing of individual practitioners authorized to sign controlled substances prescriptions prior to granting access to sign such prescriptions, two-factor authentication including a hard token separate from the computer for accessing the signing functions, requirements for the content and review of prescriptions, limited transmission provisions, requirements of pharmacy applications processing controlled substances prescriptions for dispensing, third party audits of the application providers, and internal audit functions for electronic prescription application providers and pharmacy applications. The Federal healthcare providers told DEA that the approach proposed for the private sector was inconsistent with their existing practices and did not meet the security requirements imposed on all Federal systems. The approach proposed for Federal healthcare systems was based,

therefore, on the existing Federal systems, which rely on public key infrastructure (PKI) and digital certificates to address basic security issues related to non-repudiation, authentication, and record integrity.

DEA's Concerns. DEA's proposed rule was a response to existing and potential problems that exist when prescriptions are created electronically. It is essential that the rules governing the electronic prescribing of controlled substances do not inadvertently facilitate diversion and abuse and undermine the ability of DEA, State, and local law enforcement to identify and prosecute those who engage in diversion. In this vein, DEA's primary goals were to ensure that nonregistrants did not gain access to electronic prescription applications and generate or alter prescriptions for controlled substances and to ensure that a prescription record, once created, could not be repudiated. In the case of at least some existing electronic prescription application service providers, individuals are allowed to enroll online. ASPs may ask for DEA registration and State authorization numbers, although they are not required to do so; the degree to which these are verified is at the discretion of the application provider. Similarly, application providers that sell installed applications may or may not determine whether the practitioners have valid State and DEA authorizations. Where a medical practice purchases an application or service, providers may or may not obtain this information for all practitioners in the practice.

Most of the applications appear to rely on passwords to identify a user of the application. Passwords are often described as the weakest link in security because they are easily guessed or, in healthcare settings, where multiple people use the same computers, easily observed. Where longer, more complex passwords are required by

applications as a means to increase their effectiveness, this can actually be counterproductive, as it often causes users to write down their passwords, which weakens overall security.[6] There are, in general, very limited standards for security of electronic prescription applications and no assurance that even where security capabilities exist, that they are used. For example, applications may be able to set access controls to limit who may sign a prescription, but unless those controls are set properly, anyone in a practice might be able to sign a prescription in a practitioner's name. The Certification Commission for Healthcare Information Technology (CCHIT) requires that an application have logical access controls and audit trails to gain certification, but there is no requirement that these functions be used. More than half the electronic prescription application providers certified with SureScripts/RxHub (for transmission) are not certified with CCHIT.

Even if there are logical access controls, they may not limit who can perform functions such as approving a prescription or signing it. At medical practices and even more so at hospitals and clinics, many staff members may use the same computers. The person who logged onto the application may not be the person entering prescription information later or the person who transmits the prescription. Some applications have internal audit trail functions, but whether these are active and reviewed is at the practitioner's discretion. In addition, with multiple people using computers, it is unclear that the audit trail can accurately identify who is performing actions. Except for those Federal electronic prescription applications that require practitioners to digitally sign

[6] National Institute of Standards and Technology. Special Publication 800-63-1, Draft Electronic Authentication Guideline, December 8, 2008. Appendix A.

prescriptions, none of the applications transmit any indication that a prescription was actually signed.

With multiple intermediaries moving prescriptions between practitioners and pharmacies, there is no assurance that a prescription may not be altered or added during transmission. Some intermediaries have good security, but there is no requirement for them to do so and practitioners and pharmacies have no control over which intermediaries are used. The pharmacy has no way to verify that the prescription was sent by the practitioner whose name is on the prescription or that if it was, that it was not altered after the practitioner issued it. The evidence of forgery and alteration that pharmacies use to identify illegitimate paper prescriptions do not exist in an electronic record – not only because electronic prescriptions contain no handwritten signatures, but also because electronic prescriptions are typically created from drop-down menus, which prevent or reduce the likelihood of misspelled drug names, inappropriate dosage forms and units, and other indicators of possible forgery.

The existing processes used for electronic prescriptions for noncontrolled substances, therefore, make it easy for every party to repudiate the prescription. A practitioner can claim that someone outside the practice issued a prescription in his name, that someone else in the practice used his password to issue a prescription, or that it was altered after he issued it either in transmission or at the pharmacy. Proving or disproving any of these claims would be very difficult with the existing processes. DEA and other law enforcement agencies might not be able to prove a case against someone issuing illegitimate prescriptions; equally important, practitioners might have trouble proving that they were not responsible for illegitimate prescriptions issued in their name.

Because regulations do not currently exist permitting the use of electronic prescriptions for controlled substances, there is naturally no evidence of diversion related to electronic prescriptions of these substances. That there is no evidence that other noncontrolled prescription drugs have been diverted through electronic prescriptions is not relevant for several reasons. First, there is a very limited, if any, black market for other prescription medications. Second, there is no reason for law enforcement to investigate diversion of these medications, if it occurs, because such diversion may not be illegal (this would depend on State law). Finally, the number of electronic prescriptions, including refill requests, has not been great (4 percent in 2008, according to SureScripts/RxHub).

In contrast, prescription controlled substances have always carried a significant inherent risk of diversion, both because they are addictive and because they can be sold for significantly higher prices than their retail price. The recent studies showing increasing levels of abuse of these drugs throughout the United States heightens the cause for concern. Accordingly, with controlled substances there is a considerable incentive for individuals and criminal organizations to exploit any vulnerabilities that exist to obtain these substances illegally.

The National Survey on Drug Use and Health (NSDUH) (formerly the National Household Survey on Drug Abuse) is an annual survey of the civilian, non-institutionalized, population of the United States aged 12 or older. The survey is conducted by the Office of Applied Studies, Substance Abuse and Mental Health Services Administration, of the Department of Health and Human Services. Findings from the 2008 NSDUH are the latest year for which information is currently available.

The 2008 NSDUH[7] estimated that 6.2 million persons were current users, i.e., past 30 days, of psychotherapeutic drugs--pain relievers, anti-anxiety medications, stimulants, and sedatives--taken nonmedically. This represents 2.5 percent of the population aged 12 or older. From 2002 to 2008, there was an increase among young adults aged 18 to 25 in the rate of current use of prescription pain relievers, from 4.1 percent to 4.6 percent. The survey found that about 52 million people 12 and older had used prescription drugs for non-medical reasons in their lifetime; about 35 million of these had used prescription painkillers nonmedically in their lifetime.

The consequences of prescription drug abuse are seen in the data collected by the Substance Abuse and Mental Health Services Administration on emergency room visits. In the latest data, Drug Abuse Warning Network (DAWN), 2006: National Estimates of Drug-Related Emergency Department Visits[8], SAMHSA estimates that, during that one year, approximately 741,000 emergency department visits involved nonmedical use of prescription or over-the-counter drugs or dietary supplements, a 38 percent increase over 2004. Of the 741,000 visits, 195,000 involved benzodiazepines (Schedule IV) and 248,000 involved opioids (Schedule II and III). Overall, controlled substances represented 65 percent of the estimated emergency department visits involving prescription drugs or over-the-counter drugs or dietary supplements. Between 2004 and 2006, the number of visits involving opioids increased 43 percent and the number involving benzodiazepines increased 36 percent. Of all visits involving nonmedical use

[7] Substance Abuse and Mental Health Services Administration. (2009). Results from the 2008 National Survey on Drug Use and Health: National Findings (Office of Applied Studies, NSDUH Series H-36, DHHS Publication No. SMA 09-4434). Rockville, MD. http://www.oas.samhsa.gov/nsduh/2k8nsduh/2k8Results.pdf.

[8] Substance Abuse and Mental Health Services Administration, Office of Applied Studies. Drug Abuse Warning Network, 2006: National Estimates of Drug-Related Emergency Department Visits. DAWN Series D-30, DHHS Publication No. (SMA) 08-4339, Rockville, MD, 2007. http://dawninfo.samhsa.gov/.

of pharmaceuticals, about 224,000 resulted in admission to the hospital; about 65,000 of those individuals were admitted to critical care units; 1,574 of the visits ended with the death of the patient. More than half of the visits involved patients 35 and older.

People dependent on the drugs are willing to pay a high premium to obtain them, creating a black market for these drugs. The problem of illegitimate prescriptions, which exists with paper prescriptions, is exacerbated by the speed of electronic transmissions and the difficulty of identifying an electronic prescription as invalid. A single prescription can be sent to multiple pharmacies; multiple practitioners' identities can be stolen and each identity used to issue a limited number of prescriptions to prevent a pharmacy or a State prescription monitoring program from noticing an unusual pattern. DEA's goal in the proposed rule was to address these vulnerabilities and ensure that before controlled substance prescriptions are issued electronically, the process is adequately secure to protect both DEA registrants and society.

Based on DEA's concerns, certain requirements must exist for any system to be used for the electronic prescribing of controlled substances:

- Only DEA registrants may be granted the authority to sign controlled substance electronic prescriptions. The approach must, to the greatest extent possible, protect against the theft of registrants' identities.
- The method used to authenticate a practitioner to the electronic prescribing system must ensure to the greatest extent possible that the practitioner cannot repudiate the prescription. Authentication methods that can be compromised without the practitioner being aware of the compromise are not acceptable.

- The prescription records must be reliable enough to be used in legal actions (enforcing laws relating to controlled substances) without diminishing the ability to establish the relevant facts and without requiring the calling of excessive numbers of witnesses to verify records.
- The security systems used by any electronic prescription application must, to the greatest extent possible, prevent the possibility of insider creation or alteration of controlled substance prescriptions.

Comments. DEA received 229 comments, 35 of which were copies. Twenty-one practitioner organizations, 24 pharmacy organizations, 18 States (State licensing boards of medicine and pharmacy, and three State health departments), and 19 application providers were among the commenters. Several States supported the rule as proposed, expressing concern about the security of electronic prescriptions and stating that the rule should prevent insider tampering or creation of controlled substance prescriptions. Advocacy groups concerned with drug use similarly supported the proposed rule as did a few other commenters. A number of commenters generally supported electronic prescriptions without addressing the proposed rule.

Most commenters, however, raised a substantial number of issues about various provisions of the proposed rule; their comments are addressed in detail in section IV of this preamble. On a general level, they expressed concern that the proposed requirements would prove too burdensome and would create a barrier to the adoption of electronic prescribing. They also raised two overarching issues that have affected the approach that DEA has adopted in this interim final rule.

First, the commenters noted that DEA's proposed approach addressed primarily one model for electronic prescription applications, application service providers (ASPs). In this model, the practitioner subscribes to a service and accesses, usually over the Internet, an electronic prescription application that is maintained on the ASP's servers. The ASP controls access to the application, has access to all of the records, and maintains security. The practitioner does not need to install the application or maintain servers that archive the records. Many electronic prescription application providers, particularly those that develop EHRs and hospital applications, install their software on the practitioner's computers. Once the application is installed, the electronic prescription application provider's role is limited to providing technical assistance when needed. Access control, records, and security are handled by the practitioners or their staff. Some of the proposed provisions did not work when the electronic prescription application provider is not involved in logical access control.

Second, many commenters pointed out that the technology continues to evolve, the EHR applications are still changing, and that the standards for electronic prescriptions are not mature. A number of commenters indicated that the current transmission system, which relies on a series of intermediaries to provide interoperability, may not be needed when both technology and the standards evolve. These commenters wanted DEA to provide more flexibility to be able to adjust to advancements as they occur.

III. Discussion of the Interim Final Rule

This section provides an overview of the interim final rule. As noted above, commenters raised a number of issues related to specific proposed provisions. DEA has revised the rule to address commenters' concerns and to recognize the variations in how

electronic prescription applications are implemented. In arriving at an interim final rule, DEA has balanced a number of considerations. Chief among these is DEA's obligation to ensure that the regulations minimize, to the greatest extent possible, the potential for diversion of controlled substances resulting from nonregistrants gaining access to electronic prescription applications and electronic prescriptions. At the same time, DEA has sought to streamline the rules to reduce the burden on registrants. Another of DEA's goals has been to provide flexibility in the rule so that as technologies and standards mature, registrants and application providers will be able to take advantage of advances without having to wait for a revision to the regulations. Finally, DEA has revised the rules to place requirements on either the application or on registrants so that neither DEA nor registrants are dependent on intermediaries for maintenance of information.

In response to commenters' concerns, DEA is adopting an approach to identity proofing (verifying that the user is who he claims to be) and logical access control (verifying that the authenticated user has the authority to perform the requested operation) that is different from the approach that it proposed. The interim final rule provisions related to these two steps are based on the concept of separation of duties: no single individual will have the ability to grant access to an electronic prescription application or pharmacy application. For individual practitioners in private practice (as opposed to practitioners associated with an institutional practitioner registrant), identity proofing will be done by an authorized third party that will, after verifying the identity, issue the authentication credential to a registrant. As some commenters suggested, DEA is requiring registrants to apply to certain Federally approved credential service providers (CSPs) or certification authorities (CAs) to obtain their authentication credentials or

digital certificates. These CSPs or CAs will be required to conduct identity proofing at National Institute of Standards and Technology (NIST) SP 800-63-1 Assurance Level 3, which allows either in-person or remote identity proofing. Once a Federally approved CSP or CA has verified the identity of the practitioner, it will issue the necessary authentication credential.

The successful issuance of the authentication credentials will be necessary to sign electronic controlled substance prescriptions, but possession of the credential will not be sufficient to gain access to the signing function. The electronic prescription application must allow the setting of logical access controls to ensure that only DEA registrants or persons exempted from the requirement of registration are allowed to indicate that prescriptions are ready to be signed and sign controlled substance prescriptions. Logical access controls may be by user or role-based; that is, the application may allow permissions to be assigned to individual users or it may associate permissions with particular roles (e.g., physician, nurse), then assign each individual to the appropriate role. Access control will be handled by at least two people within a practice, one of whom must be a registrant. Once the registrant has been issued the authentication credential, the individuals who set the logical access controls will verify that the practitioner's DEA registration is valid and set the application's logical access controls to grant the registrant access to functions that indicate a prescription is ready to be signed and sign controlled substance prescriptions. One person will enter the data; a registrant must approve the entry, using the two-factor authentication protocol, before access becomes operational.

DEA is allowing, but not requiring, institutional practitioners to conduct identity proofing in-house as part of their credentialing process. At least two people within the credentialing office must sign any list of individuals to be granted access control. That list must be sent to a separate department (probably the information technology department), which will use it to issue authentication credentials and enter the logical access control data. As with private practices, two individuals will be required to enter and approve the logical access control information. Institutional practitioners may require registrants and those exempted from registration under § 1301.22 to obtain identity proofing and authentication credentials from the same CSPs or CAs that individual practitioners use. The institutional practitioner may also conduct the identity proofing in-house, then provide the information to these CSPs or CAs to obtain the authentication credentials. In this last case, the institutional practitioners would be acting as trusted agents for the CSPs or CAs, under rules that those organizations set. Because DEA has made extensive changes to the requirements related to identity proofing and logical access control, DEA is seeking further comments on these issues.

As proposed, DEA is requiring in this interim final rule that the authentication credential be two-factor. Two-factor authentication (two of the following – something you know, something you have, something you are) protects the practitioner from misuse of his credential by insiders as well as protecting him from external threats because the practitioner can retain control of a biometric or hard token. Authentication based only on knowledge factors is easily subverted because they can be observed, guessed, or hacked and used without the practitioner's knowledge. In the interim final rule DEA is allowing the use of a biometric as a substitute for a hard token or a password. If a hard token is

used, it must meet FIPS 140-2 Security Level 1 for cryptographic devices or one-time-password devices and must be stored on a device that is separate from the computer being used to access the application. The CSPs and CAs may issue a new hard token or register and provide credentials for an existing token. Regardless of whether a new token is provided and activated or an existing token is registered for the signing of controlled substances prescriptions, communications between the CSP or CA and practitioner applicant must occur through two channels (e.g., mail, telephone, email).

However, while DEA is requiring in this interim final rule that the authentication credential be two-factor, DEA is seeking further comments on this issue. Specifically, DEA seeks comments in response to the following question:

- Is there an alternative to two-factor authentication that would provide an equally safe, secure, and closed system for electronic prescribing of controlled substances while better encouraging adoption of electronic prescriptions for controlled substances? If so, please describe the alternative(s) and indicate how, specifically, it would better encourage adoption of electronic prescriptions for controlled substances without diminishing the safety and security of the system.

DEA is establishing standards with which any biometric being used as one factor to sign controlled substance prescriptions must comply; however, DEA is not specifying the types of biometrics that may be used to allow for the greatest flexibility and adaptation to new technologies in the future. DEA consulted extensively with NIST in the development of these standards and has relied on their recommendations for this aspect of the rule. If a biometric is used, it may be stored on a computer, a hard token, or the biometric reader. Storage of biometric data, whether in raw or template format, has

implications for data protection and maintenance. These are considerations that should be weighed by application providers and implementers when choosing where and how biometric data may be stored. Additionally, application providers and implementers may wish to consider using open standard biometric data formats when available, to provide interoperability where more than one application provider may be providing biometric capabilities (e.g., a network that spans multiple entities) and to protect their interests. Because the use of biometrics and the standards related to their use were not discussed in the notice of proposed rulemaking, DEA is seeking further comments on these issues.

DEA is requiring that the application display a list of controlled substance prescriptions for the practitioner's review before the practitioner may authorize the prescriptions. A separate list must be displayed for each patient. All information that the DEA regulations require to be included in a prescription for a controlled substance, except the patient's address, must appear on the review screen along with a notice that completing the two-factor authentication protocol is legally signing the prescription. A separate key stroke will not be required for this statement. Registrants must indicate that each controlled substance prescription shown is ready to be signed. When the registrant indicates that one or more prescriptions are to be signed, the application must prompt him to begin the two-factor authentication protocol. Completion of the two-factor authentication protocol legally signs the prescriptions. When the two-factor authentication protocol is successfully completed, the application must digitally sign and archive at least the DEA-required information. If the practitioner is digitally signing the

prescription with his own private key[9], the application need not digitally sign the record separately, but must archive the digitally signed record. DEA is allowing any practitioner to use the digital signature option proposed for Federal healthcare systems. Unless a practitioner has digitally signed a prescription and is transmitting the prescription with the digital signature, the electronic prescription must include an indication that the prescription was signed.

The electronic prescription application must generate a monthly log of controlled substance prescriptions issued by a registrant, archive a record of those logs, and provide the logs to the practitioner. The practitioner is not required to review the monthly log.

Because the prescription information will be digitally signed when the practitioner completes the two-factor authentication protocol, the prescription need not be transmitted immediately. Information other than the information that must be digitally signed may be added to the file (e.g., pharmacy URLs) or the prescription may be reviewed (e.g., at a long-term care facility) after it is signed and before it is transmitted to the pharmacy. After the practitioner completes the authentication protocol, the information that the DEA regulations require to be included in a prescription for a controlled substance may not be modified before or during transmission.

DEA has clarified that the application may print copies of an electronically transmitted prescription if they are clearly labeled as copies, not valid for dispensing. If a

---

[9] For technical accuracy, DEA is describing the method of digitally signing as "applying the private key." The private key is a secret quantity stored on the user's token that is used in the computation of digital signatures. Digital certificates contain a related quantity called the public key, which is used to verify signatures generated by the corresponding private key. The user is not required to know, and does not enter either key. A message digest is computed by the signing software on the user's computer, and the portion of the signing function that involves the private key is automatically performed by the user's token, once the user has provided the token and a second authentication factor such as a password or PIN. From the user's perspective, the experience is similar to using an ATM card.

practitioner is notified by an intermediary or pharmacy that a transmission failed, he may print a copy of the transmitted prescription and manually sign it. The prescription must indicate that it was originally transmitted to a specific pharmacy and that the transmission failed. The pharmacy is responsible for checking to ensure that the prescription was not received electronically and no controlled substances were dispensed pursuant to the electronic prescription prior to filling the paper prescription.

DEA has also clarified that the requirement that the DEA-required contents of the prescription not be altered during transmission applies only to changes to the content (not format) by intermediaries, not to changes that may lawfully be made at a pharmacy after receipt. Pharmacy changes to electronic prescriptions for controlled substances are governed by the same statutory and regulatory limitations that apply to paper prescriptions. Intermediaries may not convert an electronic controlled substance prescription into a fax. Once a prescription is created electronically, all records of the prescription must be retained electronically.

Unless the prescription is being transmitted with a digital signature, either the last intermediary or the pharmacy must digitally sign the prescription; the pharmacy must archive the digitally signed prescription. Both the electronic prescription application and the pharmacy application must maintain an internal audit trail that records any modifications, annotations, or deletions of an electronic controlled substance prescription or when a functionality required by the rule is interfered with; the time and date of the action; and the person taking the action. The application provider and the registrants must develop a list of auditable events; auditable events should be occurrences that indicate a potential security problem. For example, an unauthorized person attempting to

sign or alter a prescription would be an auditable event; a pharmacist annotating a record to indicate a change to a generic version of a drug would not be. The applications must run the internal audit function daily to identify any auditable events. When one occurs, the application must generate a readable report for the practitioner or pharmacist. If a practitioner or pharmacy determines that there is a potential security problem, they must report it to DEA within one business day.

Application providers must obtain a third-party audit before the application may be used to create, sign, transmit, or process controlled substance prescriptions and whenever a functionality related to controlled substance prescription requirements is altered, or every two years after the initial audit, whichever occurs first. If one or more certification organizations establish procedures to review applications and determine whether they meet the requirements set forth in the DEA regulations, DEA may allow this certification to replace the third-party audit. DEA will notify registrants of any such approvals of organizations to conduct these third-party certifications through its Web site. At this time, no such certification exists for either electronic prescription or pharmacy applications, but the Certification Commission for Healthcare Information Technology (CCHIT) has developed a program for electronic prescription applications.

All records must be maintained for two years from the date on which they were created or received. Pharmacy records must be backed up daily; DEA is not specifying where back-up files must be stored.

Because DEA is allowing any registrant to use the public key infrastructure (PKI) option proposed for Federal healthcare systems, the interim final rule does not include separate requirements for these systems.

When a prescription is transmitted (outside of a closed system), it moves through three to five intermediaries between practitioners and pharmacies. Although prescriptions could be altered, added, or deleted during transmission, DEA is not regulating transmission. Registrants have no control over the string of intermediaries. A practitioner might be able to determine from his application provider which intermediaries it uses to move the prescription from the practitioner to SureScripts/RxHub or a similar service, but neither the practitioner nor the application provider would find it easy to determine which intermediaries serve each of the pharmacies a practitioner's patients may choose. Pharmacies have the problem in reverse; they may know which intermediaries send them prescriptions, but have no way to determine the intermediaries used to route prescriptions from perhaps hundreds of practitioners using different applications to SureScripts/RxHub or a similar service. DEA believes the involvement of intermediaries will not compromise the integrity of electronic prescribing of controlled substances, provided the requirements of the interim final rule are satisfied. Among these requirements is that the prescription record be digitally signed before and after transmission to avoid the need to address the security of intermediaries. DEA realizes that this approach will not prevent problems during the transmission, but it will at least identify that the problem occurred during transmission and protect practitioners and pharmacies from being held responsible for problems that may arise during transmission that are not attributable to them.

Some commenters on the NPRM claimed that the security practices of intermediaries were sufficient to protect electronic prescriptions. These practices, which are voluntary, do not address the principal threats of diversion, which occur before and

after transmission. Maintaining the integrity of the record during transmission is of little value if there is no assurance that a registrant created and transmitted the prescription or that pharmacy staff did not alter it after receipt.

DEA wishes to emphasize that the electronic prescribing of controlled substances is in addition to, not a replacement of, existing requirements for written and oral prescriptions for controlled substances. This rule provides a new option to prescribing practitioners and pharmacies. It does not change existing regulatory requirements for written and oral prescriptions for controlled substances. Prescribing practitioners will still be able to write, and manually sign, prescriptions for Schedule II, III, IV, and V controlled substances, and pharmacies will still be able to dispense controlled substances based on those written prescriptions and archive those records of dispensing. Further, nothing in this rule prevents a practitioner or a practitioner's agent from using an existing electronic prescription application that does not comply with the interim final rule to prepare a controlled substance prescription, so that EHR and other electronic prescribing functionality may be used, and print the prescription for manual signature by the practitioner. Such prescriptions are paper prescriptions and subject to the existing requirements for paper prescriptions.

IV. Discussion of Comments

A. Introduction

This section summarizes the 194 comments received to the NPRM by issue and provides DEA's responses. For each issue, DEA first summarizes the proposed rule, then presents the comments and DEA's responses. The subjects are presented in an order that tracks the process of issuing and dispensing a prescription from practitioner to pharmacy.

Issues that apply to both types of applications (e.g., third-party audits, recordkeeping) are presented once. General comments and ancillary issues are discussed at the end of this section.

B. Identity proofing and logical access control

DEA proposed that practitioners would be required to undergo in-person identity proofing, with DEA-registered hospitals, State licensing boards, or law enforcement agencies checking the identification documents. The record of the identity proofing would then have been sent to the electronic prescription application provider, which would use the information to set access controls to ensure that only practitioners eligible to issue controlled substance prescriptions were allowed to sign these prescriptions.

1. Identity proofing

Comments. Some commenters, including electronic prescription application providers and practitioner organizations, supported identity proofing, but recommended changes to the proposed rule. One physician noted that identity proofing was particularly important to prevent online enrollment without any checks on the veracity of the information submitted. Other commenters, including insurance organizations, some practitioner organizations, and some pharmacy organizations, opposed the requirement for identity proofing, stating that it would be burdensome to practitioners and a barrier to adoption of electronic prescribing. One electronic prescription application provider noted that DEA does not conduct identity proofing for issuing paper prescriptions. Several practitioner organizations and a State Board of Pharmacy stated that there was no assurance that identity proofing would reduce diversion, citing the vulnerabilities of

paper prescriptions. One pharmacy chain stated that DEA should restrict access to the database of DEA registration numbers.

DEA Response. DEA continues to believe that it is critical to the security of electronic prescribing of controlled substances that authentication credentials used to sign controlled substance prescriptions be issued only to individuals whose identities have been confirmed based on information presented in, and consistent with, the application (except for institutional practitioners; see discussion below). Without this step, nonregistrants – at a practitioner's office, at an application provider, or elsewhere – could obtain an authentication credential in a registrant's name and use it to issue illegal prescriptions. As DEA discussed in the NPRM, some existing electronic prescription application providers allow people to enroll online, with no checks on whether the person is who he claims to be. Although it is true that DEA does not require in-person identity proofing for registration and allows applications to be filed online, DEA conducts a number of checks on registration applications before issuing a registration. In addition, filing a false registration application is a Federal crime punishable by up to four years in prison under 21 U.S.C. 843. Moreover, electronic prescriptions, unlike written or oral prescriptions, lack the human elements of handwriting or the spoken voice, which a pharmacist can take into account in ascertaining whether the prescription was issued by the actual practitioner or an impostor; identity proofing serves to some degree to fill this void.

In response to comments on whether this requirement will reduce diversion, DEA is well aware of the vulnerabilities of the paper-based prescription system, but that such vulnerabilities exist does not mean that DEA should allow similar or greater

vulnerabilities with electronic prescriptions for controlled substances. A forged paper prescription provides forensic evidence of who committed the forgery and can exonerate a practitioner based on that evidence; an electronic prescription issued in a practitioner's name provides no such evidence, making it difficult for law enforcement to identify the person who issued it and difficult for the practitioner to prove that he did not. Restricting access to the CSA database would not solve the problem of patients, medical office staff, and pharmacy staff, all of whom have routine access to DEA numbers, issuing fraudulent prescriptions.

DEA recognizes that identity proofing and logical access controls (discussed below) will not stop all misuse of electronic prescription applications. Identity proofing will not prevent a registrant from issuing invalid prescriptions or allowing a staff member to issue prescriptions in his name, and it is not intended to prevent such activity. The purpose of identity proofing is to limit to as great an extent as possible the ability of nonregistrants to obtain an authentication credential and issue electronic controlled substance prescriptions under a practitioner's name.

Comments. A substantial number of commenters raised issues related to who would conduct the identity proofing. The State Boards generally objected to being asked to conduct identity proofing, asserting that they did not have the staff or resources to do so. They noted that they would need to train staff and perhaps seek legislative authority and funding to carry out this function. Other commenters doubted that hospitals or law enforcement agencies would be willing to conduct the checks or thought that DEA intended to charge for the process. Some practitioners objected to the idea of having law enforcement agencies involved. Many commenters objected to the cost of trips to a third

party and stated that it would be a barrier to adoption, particularly for practitioners who are not affiliated with a hospital, such as mid-level practitioners and dentists. Some commenters, including electronic prescription application providers, asked that other entities be allowed to conduct identity proofing (e.g., notaries, application providers, passport processing agencies, the American Association of Medical Colleges).

A long-term care facility (LTCF) organization, several information technology organizations, and an application provider suggested that DEA use existing certification authorities (CAs) that issue digital certificates and routinely conduct identity proofing as part of the enrollment process. An information technology firm suggested that DEA establish a set of common criteria under which credential issuers can become accredited, citing the Department of Defense External Certification Authority program as an example. The commenter also suggested that DEA specify that firms qualified as shared service providers by the Federal Bridge Certification Authority (FBCA) could serve as CSPs. A few commenters associated with application providers or information technology organizations asked DEA to consider remote identity proofing systems.

DEA Response. In view of the comments, DEA has revised the requirements for identity proofing to adopt an approach that does not involve parties discussed in the proposed rule. As suggested by some commenters, for individual practitioners in private practice (i.e., those practitioners not seeking access to an institutional practitioner's applications), DEA will use existing certification authorities (CAs) and similar credential service providers (CSPs) that have been approved by a Federal authority. These organizations conduct identity proofing and issue digital certificates and other identity credentials as part of their existing businesses. The standards they use to conduct identity

proofing and issue credentials are established in documents (e.g., Certificate Policies, Certificate Practice Statements, and Assurance Frameworks) that are reviewed and approved by Federal authorities and subject to third-party audits for their implementation. DEA is specifying that the identity proofing must meet NIST SP 800-63-1 Assurance Level 3 although a CA or CSP may impose higher standards.

DEA's objective is to ensure that identity proofing and the provision of two-factor authentication credentials will be done by a third party that is not involved in any other part of the electronic prescribing process. This approach is based on the concept of separation of duties, to ensure that the ability to sign controlled substance prescriptions will not depend on the action of a single entity or person. A registrant will need the two-factor authentication credential before he will be able to sign electronic prescriptions for controlled substances, but the possession of the token or tokens associated with the credential will not, itself, authorize a registrant to access the application to sign controlled substances prescriptions. Logical access control will be granted separately. Without the two-factor authentication credential, a practitioner will not be able to sign controlled substance prescriptions even if granted access.

For practitioners who are obtaining a two-factor authentication credential that does not include a digital certificate, DEA is requiring that they obtain their authentication credential from a credential service provider (CSP) that has been approved by the General Services Administration Office of Technology Strategy/Division of Identity Management to conduct identity proofing that meets NIST Sp 800-63-1 Assurance Level 3 or above. For practitioners obtaining a digital certificate, DEA is requiring that they obtain the digital certificate from a certification authority that is cross-

certified with the Federal Bridge Certification Authority (FBCA) at a basic assurance level or higher and that conducts identity proofing at NIST SP 800-63-1 Assurance Level 3 or above. DEA believes that shared service providers would be too restrictive and believes that the approach it is implementing provides greater flexibility for the regulated industry.

DEA is not dictating how a CSP or CA conducts identity proofing. The standards for identity proofing are set by the Federal Bridge Certification Authority (FBCA) or the General Services Administration in their certificate policies and frameworks and in NIST SP 800-63-1. Level 3 requires either in-person identity proofing based on checking government-issued photographic identification or remote identity proofing. For in-person identity proofing, Level 3 requires the examination of a government-issued photographic identification, which must be verified with either the issuing agency, credit bureaus, or other similar databases. The verification must confirm that the name, date of birth, and address listed in the application for the credential are consistent with the information in other records checked. The person checking the identification must compare the person with the photograph, record the identification number, address (if listed), and date of birth. If the identification is valid, the issuing organization may authorize or issue the credential and send notice to the address of record; if the identification or other records checked do not confirm the address listed in the application (as may happen if the person has recently moved), the organization must issue credentials in a manner that confirms the address of record (the address of record is the address listed in the application).

For remote identity proofing, Level 3 requires a valid government-issued identification number and a financial account number. These numbers must be

confirmed via record checks with either the issuing agency or institution or through credit bureaus or similar databases. The check must confirm that the name, address, date of birth, and other personal information in the records are consistent with the application and sufficient to identify a unique individual. The address or telephone number must be confirmed by issuing the credential in a manner that confirms the ability of the applicant to receive communications at the listed address or number. DEA notes that CAs and CSPs may conduct more extensive remote identity proofing and may require additional information from applicants. DEA believes that the ability to conduct remote identity proofing allowed for in Level 3 will ensure that practitioners in rural areas will be able to obtain an authentication credential without the need for travel. DEA expects that application providers will work with CSPs or CAs to direct practitioners to one or more sources of two-factor authentication credentials that will be interoperable with their applications. DEA is seeking comment on this approach to identity proofing.

DEA is not requiring the CSP or CA to check DEA registrations or State authorizations to practice or dispense controlled substances as part of the identity-proofing process; these will be checked as part of logical access control, as discussed in the next section. DEA decided to have checks for the DEA registration, authorization to practice, and authorization to dispense controlled substances for individual practitioners handled separately from identity proofing for three reasons. First, the information that is used to verify identity may not be the information associated with a DEA registration. Government-issued photographic identifications and credit cards usually are associated with home addresses and, perhaps, Social Security numbers; DEA registrations are usually associated with business locations and, in some cases, taxpayer identification

numbers. In addition, the registration database that DEA makes available through the National Technical Information Service does not include this personal information, so that a CA or CSP would have to contact DEA for each applicant. Second, some practices or application providers may want some or all of the nonregistrants on the staff to obtain authentication credentials so that there will be only one method of authenticating to the application. The possession of a two-factor authentication credential would not, in these cases, distinguish between those who can sign controlled substance prescriptions and those who cannot. Third, the decision to grant access to the functions that allow a practitioner to indicate that a prescription is ready for signing and to sign controlled substance prescriptions is based on whether the person is a DEA registrant, not on the possession of a two-factor authentication credential. The two-factor authentication credential is a necessary, but not a sufficient, condition for signing a controlled substance prescription. It is logical, therefore, to require the people who set logical access controls, rather than those who conduct identity proofing, to check the DEA and State authorizations to practice and, where applicable, authorizations to dispense controlled substances of prescribing practitioners.

Comments. One medical group association and a healthcare system recommended that the larger practices be allowed to conduct the identity proofing themselves as they already conduct Level 4 identity proofing when they issue credentials.

DEA Response. In view of the comments, DEA has expanded upon the proposed rule to allow institutional practitioners, which are themselves DEA registrants, to conduct the identity proofing for any individual practitioner whom the institutional practitioner is granting access to issue prescriptions using the institution's electronic prescribing

application. Because institutional practitioners have credentialing offices, the interim final rule allows those offices to conduct in-person identity proofing, which they can do as part of their credentialing process. DEA is not requiring institutional practitioners to meet the requirements of NIST SP 800-63-1 for identity proofing. As some commenters stated, these institutions already conduct extensive checks before they credential a practitioner. The interim final rule simply requires that before they issue the authentication credential they check the person's government-issued photographic identification against the person presenting it. They must also check State licensure and DEA registrations, where applicable, but they do this as part of credentialing and do not need to repeat the checks for practitioners whom they have already credentialed.

The rule only allows institutional practitioners to conduct in-person identity proofing, not remote identity proofing. There are two reasons for this limitation. First, the practitioners will be visiting the institution on a regular basis so the burden should be relatively low. Second, most institutional practitioners may not have the ability or desire to conduct the credit and other background checks that are part of remote identity proofing at NIST Levels 2 and 3. DEA recognizes that in some large systems, the credentialing office may be at a central location and many staff may work at other locations. In those cases, the institutional practitioner can decide whether to have the staff visit the central location or send someone from the credentialing office to the other locations to conduct the identity proofing. DEA notes that this issue will arise only during the initial enrollment of previously credentialed practitioners. After that, practitioners being newly credentialed by an institution can undergo identity proofing when and where they are credentialed. The rule also requires that the credentialing office

check the DEA and State authorizations to practice and, where applicable, authorizations to dispense controlled substances because this check should be part of their standard credentialing process.

Under the rule, the institutional practitioner may issue the two-factor authentication credentials itself or obtain them from a third party, which will have to be a CSP or CA that meets the criteria specified above. In the latter case, the institutional practitioner could have each practitioner apply for the two-factor credential himself, which would entail undergoing identity proofing by the CSP or CA. Alternatively, the institutional practitioner can serve as a trusted agent for the third party. Trusted agents conduct part of the identity proofing on behalf of the CSP or CA and submit the information for each person along with a signed agreement that specifies the trusted agent's responsibilities. DEA emphasizes that institutional practitioners are allowed, but not required, to conduct identity proofing. If an institutional practitioner (e.g., a small hospital or clinic) decides to have each practitioner obtain identity proofing and the two-factor authentication credential on his own, as other individual practitioners do, that is permissible under the rule. DEA is seeking comment on this approach to identity proofing by institutional practitioners.

Comments. An intermediary, a pharmacist organization, and a State asked whether practitioners would need to undergo identity proofing more than once if they used multiple electronic prescription applications. An application provider and a practitioner organization asked if the identity proofing needed to be revalidated every year. Several commenters asked about the need to obtain separate authentication credentials if the practitioner holds multiple DEA numbers.

DEA Response. Identity proofing is required to obtain a two-factor authentication credential. If a practitioner uses multiple applications (e.g., at his practice and at a hospital), he may need to obtain separate authentication credentials, based on the following considerations. A practitioner will need to undergo identity proofing for each such credential that he needs unless the applications he wishes to use require authentication credentials from the same CSP or CA; in that case, the CSP or CA will determine whether a single application for identity proofing and issuance of the authentication credential can serve as a basis for issuing multiple credentials. It may also be possible that multiple applications will accept the same two-factor authentication credential. For example, if a practitioner obtains a digital certificate from an approved CA, he may be able to use it to digitally sign prescriptions on multiple applications, if they accept digital signatures. For those practitioners who use more than one DEA registration to issue controlled substance prescriptions, DEA is not requiring a practitioner to have a separate authentication credential based solely on the fact that he uses more than one DEA registration. As for the need for revalidation of identity proofing, those periods will be set by the CSP or CA.

Comments. Practitioner organizations asked if practitioners will be charged for the identity proofing.

DEA Response. DEA expects that the CSP or CA will charge for the issuance of a two-factor authentication credential, which will generally include the cost of identity proofing. Whether practitioners will pay directly or through the application provider will be a business decision on the part of application providers.

Comments. A practitioner organization expressed concern with the proposed rule language that referenced "State licenses" because some States do not issue licenses to mid-level practitioners.

DEA Response. DEA agrees with this commenter and has revised the language in the interim final rule to refer to State authorization to practice and State authorization to dispense controlled substances.[10]

2. Access Control

In the NPRM, DEA proposed that the identity proofing document had to be submitted to the application provider, which would then check the DEA registration and State authorizations to practice, and set access controls. DEA also proposed that the application providers check DEA registration status weekly and revoke authentication credentials if practitioners' registrations had been terminated, revoked, or suspended.

Comments. A LTCF organization stated that any electronic prescribing application must have, at its core, control over access rights. A practitioner organization also emphasized the need to limit access to signing authority within an application. An electronic prescription application provider stated that it did not set access controls for the applications it sells and installs at medical practices. Although its applications have logical access controls, the practice administrator is responsible for setting the controls. The application provider is not involved in the process.

[10] Under the CSA, every person who dispenses a controlled substance must have a DEA registration, and may only dispense controlled substances to the extent authorized by his registration, unless DEA has by regulation, waived the requirement of registration as to such person. 21 U.S.C. 822(a)(2), 822(b), 822(d). To be eligible to obtain a DEA registration, a practitioner must be licensed or otherwise authorized by the State or jurisdiction in which he practices to dispense controlled substances. 21 U.S.C. 802(21), 823(f), 824(a)(3).

DEA Response. In its proposed rule, DEA did not adequately differentiate between authentication, authorization, and access. NIST, in its special publication SP 800-12, provides the following description of these three steps:

> Access is the ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection).
> Authorization is the permission to use a computer resource. Permission is granted, directly or indirectly, by the application or system owner.
> Authentication is proving (to some reasonable degree) that users are who they claim to be.

NIST SP 800-12 further states:

> Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls). Computer-based access controls are called logical access controls. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. These controls may be built into the operating system, may be incorporated into applications programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages.[11]

DEA has revised its approach to access control to remove the application provider and its staff from direct involvement in the process. Instead, the interim final rule will require that the application must have the capability to set logical access controls that limit access to the functions for indicating a prescription is ready for signing and for signing the prescription to DEA registrants. The interim final rule will also limit access to setting these logical access controls. The application may set logical access controls on an individual basis or on roles. If the logical access controls are role-based, one or more roles will have to be limited to individuals authorized to prescribe controlled

[11] National Institute of Standards and Technology. Special Publication 800-12 An Introduction to Computer Security– The NIST Handbook, Chapter 17; October, 1995. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter17-printable.html

substances. This role may be labeled "DEA registrant" or physician, dentist, nurse practitioner, etc., provided the role is limited to those authorized to issue controlled substance prescriptions. For an individual practitioner who is an agent or employee of an institutional practitioner, and who has been authorized to prescribe controlled substances under the registration of the institutional practitioner pursuant to 21 CFR 1301.22(c), if logical access controls are role-based, one role will have to be "authorized to sign controlled substance prescriptions." (Other methods of setting logical access controls that NIST cites – location or time – do not appear to be relevant, although applications or users may add such limits based on their own concerns.)

The application logical access control capability must require that data entry of authorizations for setting logical access controls and the functions limited to registrants (indicating that a controlled substance prescription is ready for signing and signing a controlled substance prescription) involve two people. The requirement for two people to be involved in such data entry is frequently used to protect applications from internal security threats. If a person is able, through the use of false identity documents, to obtain a two-factor authentication credential in a registrant's name, he will still not be able to sign controlled substance prescriptions unless he is granted access, by two people (one of whom is a registrant). The interim final rule does not specify in detail how the application must be structured to ensure that two people concur with the data entry; rather, the rule simply requires that the application must not accept these logical access controls without the action of two parties. For example, a small practice with two registrants neither of whom is expecting to leave may decide that only the registrants will perform this function, which may occur only at the initial installation or upgrade of an

electronic prescription application to comply with controlled substance prescription requirements. In large practices, the registrants might find it beneficial to allow nonregistrants, such as a practice information technology administrator, to administer logical access controls in conjunction with a registrant.

The interim final rule requires that at least one of the people assigned the role of administering logical access control must verify that any registrant granted authorization to indicate that a prescription is ready for signing and to sign controlled substance prescriptions has a valid DEA registration, a State authorization to practice and, where applicable, a State controlled substance authorization. In small practices, this verification may require nothing more than checking expiration dates on the practitioners' DEA Certificate of Registration and State authorization(s), unless there is reason to question the current validity. In larger practices, verification may take more time. Individual registrations can be checked online at DEA's Web site at www.deadiversion.usdoj.gov/ by clicking on the Registration Validation button on the left side of the Web page.

Once DEA registration and State authorization to practice and State authorization to dispense controlled substances have been verified, two people must be involved in entering the data to the application to identify those people authorized to indicate that a prescription is ready for signing and to sign controlled substance prescriptions; those two people are also involved in entering data to the application to identify people whose authorization has been revoked. The first person must enter the data. A registrant must then use his two-factor authentication credential to provide the second approval. The application must ensure that until the second approval occurs, logical access controls for controlled substance prescription functions cannot be activated or altered. DEA

recognizes that some solo practitioners may not have other employees although it seems unlikely that they do not have at least part-time help for office management and back office functions. DEA is not requiring that the second person be an employee, simply that there be two people involved and that the persons involved be specifically designated by the practitioner(s). For such solo practitioners and for many small practices, logical access controls may need to be set only once because they will usually be set or changed only with staff turnover.

All entries and changes to the logical access controls for setting the controls and for the controlled substance prescription functions must be defined as auditable events and a record of the changes retained as part of the internal audit trail. DEA is seeking comment on this approach to logical access control for individual practitioners.

Logical access must be revoked whenever any of the following occurs: a DEA registration expires without renewal, or is terminated, revoked, or suspended; the registrant reports that a token associated with the two-factor authentication credential has been lost or compromised; or the registrant is no longer authorized to use the practice's application. DEA anticipates that for most practices, logical access controls will be set and changed infrequently, usually when a new registrant joins the practice or a registrant leaves. Even in larger practices, changes to authorizations are likely to occur relatively infrequently.

DEA recognizes that application service providers (ASPs) may currently set access controls, to the extent that they do, at the ASP level and that the interim final rule may require them to reprogram some of their security controls. DEA believes these steps are necessary to ensure that a registrant is involved in the process of setting logical access

controls and that these cannot be set or changed without the concurrence of a registrant. If registrants submitted a list of people to be authorized to perform the controlled substance prescription functions to an ASP, there would need to be a process to ensure that the list was from a legitimate source (e.g., notarization), which could be cumbersome, particularly for larger practices where the list may change more frequently than is the case for small practices. In addition, the responsibility for data entry would then rest with ASP staff, who will not have the same degree of interest in protecting registrants from the misuse of the applications as the registrants themselves have.

For institutional practitioners, the setting of logical access controls will necessarily be somewhat different because the registrant is not an individual. The principle, however, is the same. Identity proofing must be separate from setting logical access controls; two individuals must be involved in each step. The interim final rule therefore requires that two individuals from the credentialing office provide the part of the institution that controls the computer applications with the names of practitioners authorized to issue controlled substance prescriptions. The entry of the data will also require the involvement of two individuals. The institutional registrant is responsible for designating and documenting individuals or roles that can perform these functions. Logical access must be revoked whenever any of the following occurs: the institutional practitioner's or, where applicable, individual practitioner's DEA registration expires without renewal, or is terminated, revoked, or suspended; the practitioner reports that a token associated with the two-factor authentication credential has been lost or compromised; or the individual practitioner is no longer authorized to use the institutional

practitioner's application. DEA is seeking comment on this approach to logical access control for institutional practitioners.

Comments. An application provider to a major healthcare system agreed that access controls were needed, but noted that in a large healthcare system this is complex because of the variety of practitioners involved and will take time to implement.

DEA Response. The interim final rule does not require applications to distinguish which schedules of controlled substances a registrant is authorized to prescribe. Practitioners are responsible for knowing which schedules they may prescribe; if a practitioner prescribes beyond the extent authorized by his registration, he is dispensing in violation of the CSA.[12] In addition, asking applications to distinguish among all the variations of prescribing authority may add unnecessary complication to applications that will mostly be used by practitioners who are authorized to prescribe all Schedule II, III, IV, and V substances. This approach should reduce some of the complexity in programming logical access controls because the application providers will not need to distinguish among DEA registrants. DEA also notes that the 2009 security survey of the Health Information and Management Systems Society (HIMSS) indicated that all of the 196 healthcare systems surveyed have established user access controls.[13]

Comments. Several application providers objected to the proposed requirement that they check DEA registration status weekly.

DEA Response. Because application providers are no longer responsible for controlling access, DEA has removed this requirement in the interim final rule. People

---

[12] 21 U.S.C. 822(b), 841(a)(1).
[13] Healthcare Information and Management Systems Society. 2009 HIMSS Security Survey, November 3, 2009. http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf

within a practitioner's office or an institutional practitioner will be familiar with any issues related to the status of a DEA registration. They will have access to the expiration date of the DEA registration and State authorization(s) to practice and, where applicable, to dispense controlled substances and be able to check with the practitioner to ensure that the registration has been renewed. If a practitioner is subject to suspension or revocation, other registrants in the practice or the institutional practitioner are likely to be aware of the legal problems and can revoke access control.

DEA recognizes that this approach will not prevent a registrant in solo practice from continuing to issue controlled substances prescriptions under an expired, terminated, suspended, or revoked registration. However, it is already clear under existing law and regulations that a practitioner who prescribes or otherwise dispenses controlled substances beyond the scope of his registration is committing a violation of the CSA and subject to potential criminal prosecution, civil fine, and loss of registration. Any practitioner who would use his two-factor authentication credential to issue prescriptions after he is legally barred from doing so would be creating evidence of such criminal activity. As discussed above, the purpose of identity proofing and access control is to prevent nonregistrants from gaining the ability to issue controlled substance prescriptions.

C. Authentication Protocols

Authentication protocols are classified by the number of factors they require. NIST and others recognize three factors: something you know, something you have, and something you are. Combinations of user IDs and passwords are one-factor because they require only information that you know. A standard ATM uses two-factor – something

you know (a personal identification number (PIN)) and something you have (bank card). DEA proposed that practitioners be required to use a two-factor authentication protocol to access the electronic prescription application to sign controlled substance prescriptions. DEA proposed that one factor would have to be a hard token that met NIST SP 800-63 Level 4 and that the cryptographic module would have to be validated at Federal Information Processing Standard (FIPS) 140-2 Security Level 2 overall and Level 3 security.

Comments. Three information technology firms asserted that two-factor authentication is not common. They suggested that a clear 'audit log' be generated upon the provider authentication, prescription approval, transmission of prescription, and successful prescription transmittal. They suggested that this audit log should be in the form defined by Healthcare Information Technology Standards Panel (HITSP) T15 "Collect and Communicate Security Audit Trail Transaction." Other commenters noted that the Certification Commission for Healthcare Information Technology (CCHIT) does not require two-factor authentication and has only listed it as a possibility for its 2010 standard. A State Board of Pharmacy supported two-factor authentication, stating that concerns expressed by some members of industry about the added time to complete two-factor authentication are misplaced. It said that the two-factor authentication will take a minimal amount of time compared to the time it takes to move through the multiple screens used to create a prescription in most applications.

DEA Response. DEA agrees that CCHIT does not yet require two-factor authentication. Two-factor authentication is roadmapped by CCHIT in 2010 and beyond. DEA emphasizes, however, that an audit log will not provide any assurance of who

issued a prescription. The commenters appear to have confused logical access control with authentication. The problem DEA is addressing with the requirement for two-factor authentication credentials is not that someone may use their own authentication credential to alter or create a prescription, but that a nonregistrant will use a registrant's authentication credential to create and sign a prescription. If a nonregistrant has been able to use a registrant's authentication credential, the audit trail will incorrectly indicate that the registrant was responsible for the prescription. DEA believes that use of two-factor authentication limits this possibility.

As commenters indicated, single-factor authentication usually means passwords alone or in combination with user IDs. NIST states in it special publication SP 800-63-1: "… the ability of humans to remember long, arbitrary passwords is limited, so passwords are often vulnerable to a variety of attacks including guessing, use of dictionaries of common passwords, and brute force attacks of all possible password combinations. … all password authentication mechanisms are vulnerable to keyboard loggers and observation of the password when it is entered." NIST also states that "… many users, left to choose their own passwords will choose passwords that are easily guessed and even fairly short[.]"[14] This problem is exacerbated in healthcare settings where multiple people may use the same computers and work in close proximity to each other. Even if other staff cannot guess the password, they may have many opportunities to observe a practitioner entering the password. Strong passwords (combinations of 8 or more letters, numbers, and special characters) are hard to remember and are often written down. None of these strategies alters the ability of others in a healthcare setting to observe the password.

[14] National Institute of Standards and Technology. Special Publication 800-63-1, Draft Electronic Authentication Guideline, December 8, 2008, Appendix A. http://csrc.nist.gov/Publications/PubsSPs.html

NIST, in its draft guidance on enterprise password management (SP 800-118) states the following:

> Organizations should be aware of the drawbacks of using password-based authentication. There are many types of threats against passwords, and most of these threats can only be partially mitigated. Also, users are burdened with memorizing and managing an ever-increasing number of passwords. However, although the existing mechanisms for enterprise password management can somewhat alleviate this burden, they each have significant usability disadvantages and can also cause more serious security incidents because they permit access to many systems through a single authenticator. Therefore, organizations should make long-term plans for replacing or supplementing password-based authentication with stronger forms of authentication for resources with higher security needs.[15]

DEA remains convinced that single-factor authentication is insufficient to ensure that a practitioner will not be able to repudiate a prescription he signed.

Comments. Although only a few commenters opposed two-factor authentication, believing that passwords were sufficient, most comments DEA received on the issue raised substantial concerns about the details of the proposed rule on this subject. These concerns focused on the requirement for a hard token and the security levels proposed.

A practitioner organization, a hospital organization, a pharmacy association, a health information technology organization, a healthcare system, other medical associations, and a number of application providers asked DEA to allow the use of biometrics as an alternative to a hard token. The practitioner organization stated that a second authentication at the time of transmission is reasonable given the potential for unintentional or intentional failure to have only authorized prescribers actually transmit the prescription. That commenter asserted that the key is to view authentication as

---

[15] National Institute of Standards and Technology. Special Publication 800-118, Guide to Enterprise Password Management (draft), April 2009; http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf.

having many highly acceptable approaches and requiring that a certain strength of authentication be the outcome, but not prescribe the exact method by which that authentication is generated. A health information technology organization asserted that the Association of American Medical Colleges uses a fingerprint biometric strategy to permanently identity proof all future physicians at the time they take their Medical College Admission Test (MCAT). An application provider noted that biometric identifiers will limit unauthorized access to electronic prescription applications and ensure non-repudiation with absolute certainty; the commenter asserted that these applications cannot be compromised without the practitioner's knowledge. The commenter noted that biometric identifiers cannot be misplaced, loaned to others or stored in a central location for use by other persons. The commenter noted, however, that the technology may not be ready to deploy in a scalable, cost-effective way at this time.

DEA Response. DEA agrees with these commenters and has revised the interim final rule to allow the use of a biometric as a second factor; thus, two of the three factors must be used: a biometric, a knowledge factor (e.g., password), or a hard token. While DEA is uncertain about the extent to which existing biometric readers will be used in healthcare settings, DEA believes it is reasonable to allow for such technology because the technology is likely to improve. The HIMSS 2009 security survey indicated that 19 percent of the 196 healthcare systems surveyed use biometric technologies as a tool to provide security for electronic patient data; the HIMSS 2009 leadership survey of larger healthcare systems found that 18 percent used biometrics as a tool to provide security for

electronic patient data, but 36 percent indicated that they intended to do so.[16] The 2009 security survey also found that 33 percent of the systems already use two-factor authentication for security.

DEA is establishing several requirements for the use of biometrics, and for the testing of the software used to read the biometrics. DEA is establishing these standards after extensive consultation with NIST, and based on NIST recommendations. A discussion of these requirements follows.

- The biometric subsystem must operate at a false match rate of 0.001 or lower.

The term "false match rate" is similar to the term "false accept rate" – it is the rate at which an impostor's biometric is falsely accepted as being that of an authorized user. DEA is not establishing a false non-match (rejection) rate; while users may be interested in this criterion, DEA does not have an interest in setting a requirement for a tolerance level for false rejections for electronic prescription applications.

- The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the required false match rate specified (0.001) or a lower false match rate. This testing must be performed by the National Institute of Standards and Technology (NIST) or another DEA-approved (government or non-government) laboratory.

This criterion is designed to ensure that an independent third-party has tested the software and has determined its effectiveness on a sequestered data set that is large enough for high confidence in the results, which will be made publicly available for consumers. DEA believes that the requirement to have the biometric software tested by

[16] Healthcare Information and Management Systems Society. 2008 HIMSS Security Survey, October 28, 2008. HIMSS, 20th Annual 2009 HIMSS Leadership Survey, April 6, 2009. http://www.himss.org

an independent third party, as discussed further below, will provide greater assurance to electronic prescription application providers and practitioners that the biometric subsystem being used, in fact, meets DEA's requirements. NIST currently lists technologies which it has tested and their rates of performance at the following URLs: http://fingerprint.nist.gov for fingerprint testing, http://face.nist.gov for facial testing, and http://iris.nist.gov for iris testing.

- The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST Special Publication 800-76-1, if they exist for the biometric modality of choice.

This requirement specifies minimum requirements for the performance of the device that is used to acquire biometric data (usually an image), whereas the prior requirements relate to the software used to compare biometric samples to determine if a user is who he claims to be. NIST Special Publication 800-76-1[17] describes technical acquisition and formatting specifications for the biometric credentials of the PIV system. Section 4.2 covers sensor specifications for fingerprint acquisition for the purpose of authentication; Section 8.6 covers conformance to this specification. Section 5.2 covers both format and acquisition specifications for facial images. While the format requirements for PIV will not be required by DEA here, the normative requirements for facial image acquisition establish minimum criteria for automated face recognition, specifically the "Normative Notes," numbers 4 through 8 under Table 6. DEA also recommends using the normative values for PIV conformance in Table 6 rows 36 through

[17] National Institute of Standards and Technology. Special publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007. http://csrc.nist.gov/publications/PubsSPs.html

58 for frontal facial image acquisition. Currently, specifications exist only for fingerprint and face acquisitions.

DEA wishes to emphasize that the use of SP 800-76-1 does not imply that all requirements related to Federally mandated Personal Identity Verification cards apply in this context, only those specified for biometric acquisition for the purposes of authentication. PIV goes beyond this application, in that it has additional requirements for fingerprint registration (or enrollment) suitable for a Federal Bureau of Investigation background check, and the PIV credential has interoperability requirements that will not necessarily apply to users of controlled substance electronic prescription applications.

- The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.

This criterion is intended to add to the security of the biometric factor by physically controlling access to the biometric device to reduce the potential for spoofing.

- The biometric subsystem must store device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication.

Within this context, enrollment is the process of collecting a biometric sample from a new user and storing it (in some format) locally, on a network, and/or on a token. These enrolled data are stored for the purpose of future comparisons when someone (whether the genuine user or an impostor) attempts to log in. To help ensure that log-in

attempts are being initiated by the genuine user (as opposed to a spoofed biometric), this requirement in combination with the above requirement increase the difficulty for an impostor to spoof a biometric and remotely issue an unlawful prescription.

- The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local.
- If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:
    - Cryptographically source authenticated;
    - Combined with a random challenge, a nonce, or a timestamp to prevent replay;
    - Cryptographically protected for integrity and confidentiality;
    - Sent only to authorized systems.

The above requirements are to ensure the security and integrity for this authentication factor (a biometric), ensuring any data related to the biometric subsystem (biometric patterns and results of comparisons) are sent from an authorized sourced to an authorized destination and that the message was not tampered with in transit. Additionally, cryptographic protection of the biometric data addresses an aspect of the user's interests in confidentiality of personal data.

The easiest way to meet the above requirements when authentication is not local is to run a client authenticated TLS connection or a similar protocol between the endpoints of any remote communication carrying data subject to the above requirements. Another possible solution that may be used is server authenticated TLS in combination with a secure HTTP cookie at the client that contains at least 64 bits of entropy.

DEA also recognizes that biometrics application providers have a vested interest in either selling their applications directly to practitioners or electronic prescription application providers, or partnering with those electronic prescription application providers to market their applications. Therefore, as discussed above, to provide practitioners and electronic prescription application providers with an objective appraisal of the biometrics applications they may purchase and use, DEA is requiring independent testing of those applications. This testing is similar to the third-party audits or certifications of the electronic prescription and pharmacy applications DEA is also requiring. Testing of the biometric subsystem must have the following characteristics:

- The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.

DEA wishes to ensure that the testing body is independent and neutral. As noted previously, tests may be conducted by NIST, or DEA may approve other government or nongovernment laboratories to conduct these tests.

- Test data are sequestered.
- Algorithms are provided to the testing laboratory (as opposed to scores).

To the extent possible, independent testing should provide an unbiased evaluation of its object of study, which should yield repeatable, generalizable results. The above two requirements reflect the principle behind independent testing. If test participants had access to the test data used in an evaluation, they would have the opportunity to tune or augment their algorithms to maximize accuracy on that data set, but would likely fail to give a fair assessment of the algorithm's performance. Therefore, test data should not be made public before the testing period closes, and if test data are sequestered, algorithms

must be provided to the independent testing laboratory for the experiment(s) to be conducted. Additionally, the latter requirement permits the independent testing laboratory to produce the results itself that are ultimately used to characterize performance.

- The operating point(s) corresponding with the false match rate specified (0.001), or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.

As discussed above, testing should yield results that are repeatable. The resulting measurements of an evaluation should have a reasonably high degree of reliability. A confidence level of 95% or greater will characterize the values from an evaluation as reliable for this context.

- Results are made publicly available.

The provision of testing results to the public, either through a Web site or other means, will help to ensure transparency of the testing process and of the results. Such transparency will provide greater opportunity for interested electronic prescription application providers and others to compare results between biometrics application providers to find the biometric application that best meets their needs.

DEA recognizes the need for assurance that a captured biometric sample is obtained from a genuine user - and not a spoofed copy, particularly in unattended applications such as electronic prescriptions for controlled substances, where many users may have access to computers that contain electronic prescription applications. Liveness detection is a tool that some biometric vendors have developed to address this issue. However, since this is an active area of research that has not been standardized, DEA is

not setting a specific requirement for liveness detection at this time, but will reconsider this tool in the future as industry standards and specifications are developed.

DEA emphasizes that the use of biometrics as one factor in the two-factor authentication protocol is strictly voluntary, as is all electronic prescribing of controlled substances. As noted previously, DEA wishes to emphasize that these standards do not specify the types of biometrics that may be acceptable. Any biometric that meets the criteria specified above may be used as the biometric factor in a two-factor authentication credential used to indicate that prescriptions are ready to be signed and sign controlled substance prescriptions. DEA, after extensive consultation with NIST, has written these criteria to be as flexible as possible to emerging technologies, allowing new biometrics systems to develop in the future that meet these criteria.

Because the use of biometrics and the standards related to their use were not discussed in the notice of proposed rulemaking, DEA is seeking further comment on these issues. Specifically, DEA is seeking comments in response to the following questions:

- What effect will the inclusion of biometrics as an option for meeting the two-factor authentication requirement have on the adoption rate of electronic prescriptions for controlled substances, using the proposed requirements of a password and hard token as a baseline? Do you expect the adoption rate to significantly increase, slightly increase, or be about the same? Please also indicate why.
- Is there an alternative to the option of biometrics which could result in greater adoption by medical practitioners of electronic prescriptions for controlled

substances while also providing a safe, secure, and closed system for prescribing controlled substances electronically? If so, please describe the alternative(s) and indicate how, specifically, it would be an improvement on the authentication requirements in this interim rule.

Also, based on the comments received, it appears that a number of commenters may have already implemented biometrics as an authentication credential to electronic applications. DEA is seeking information from commenters on their experiences implementing biometric authentication. DEA seeks the following information:

- Why was the decision made to adopt biometrics as an authentication credential? Why was the decision made to adopt biometrics as opposed to another option? What other options were considered?
- What are biometrics as an authentication credential used for (e.g., access to a computer, access to particular records, such as patient records, or applications)?
- How many people in the practice/institution use biometric authentication (number and percentage, type of employee – practitioners, nurses, office staff, etc.)?
- What types of biometric authentication credentials are used (e.g., fingerprint, iris scan, hand print)?
- How are the biometrics read, and what hardware is necessary (e.g., fingerprint readers built into keyboards or mouses, on-screen biometric readers, external readers attached to computers)?
- Is biometric authentication used by itself or in combination with a user ID or password?

- How are biometric readers distributed (e.g., at every computer workstation, at certain workstations based on location, allocated based on number of staff)?
- Was the adoption of biometrics part of installation of a new system or an addition to existing applications?
- How long did the implementation process take? Was the time related to implementing biometrics or other application installation issues?
- Which parts of the biometric implementation were completed without difficulty?
- What challenges were encountered and how were they overcome?
- Were workflows affected during or after implementation and, if so, how were they affected and for how long?
- How do the users feel about the use of biometrics as an authentication credential?
- Has the use of biometric authentication improved or slowed workflows? If so, how?
- Has the use of biometric authentication improved data and/or network security?
- What other benefits have been realized?

Comments. A practitioner organization recommended that the second factor be eliminated when a biometric authentication device is used.

DEA Response. DEA believes that any authentication protocol that uses only one factor entails greater risk than a two-factor authentication protocol. While DEA recognizes the strength that biometrics provide, biometric readers themselves are not infallible. They can falsely accept a biometric, or purported biometric, that does not correspond to the biometric associated with a particular user. Requiring two-factor authentication, regardless of the factors used (Something you know, something you have,

and something you are), ensures a strong authentication method, which DEA believes is necessary to sign electronic prescriptions for controlled substances.

Comments. Some physician and pharmacy organizations objected to hard tokens, asserting that they are inconvenient, impractical, easily lost or shared, and generally not secure enough. They suggested tap-and-go proximity cards because, they asserted, such cards would be more cost effective. These physician organizations further noted that hospital security systems may bar the use of certain hard tokens. One application provider indicated that it had tried one-time-password devices in an application used for electronically prescribing noncontrolled substances and found they discouraged use of the application. Two large healthcare systems suggested alternative challenge-response methods as well as biometrics as another approach for closed systems.

Other commenters objected to the requirement for Level 4 security for the hard token. They noted that relatively few devices that are validated by Federal Information Processing Standards (FIPS) meet Level 4. One application provider stated that DEA's description in the proposed rule is more like Level 3 with a hard token. It asserted that Level 4 would mean that any user of the application, not just practitioners signing controlled substance prescriptions, would need Level 4 tokens. Some commenters further asserted that few devices meet FIPS 140-2 Security Level 3 for physical security. An intermediary stated the current NIST SP 800-63-1 draft definition is different from the original SP 800-63 definition; the commenter indicated that SP 800-63-1 does not require that approved cryptographic algorithms must be implemented in a cryptographic module validated under FIPS 140-2. Thus, the commenter believed, the requirements according to this new draft SP 800-63-1 could be implemented more easily.

DEA Response. DEA has revised this rule to allow the use of a hard token that is separate from the computer being accessed and that meets FIPS 140-2 Security Level 1 security or higher. Proximity cards that are smart cards with cryptographic modules could serve as hard tokens. The FIPS 140-2 requirements for higher security levels generally relate to the packaging of the token (tamper-evident coatings and seals, tamper-resistant circuitry). DEA does not consider this level of physical security necessary for a hard token.

Contrary to the intermediary's statement, NIST SP 800-63-1 does require that cryptographic modules be FIPS 140-2 validated. NIST SP 800-63-1 requires the following for one-time-password devices: "Must use approved block cipher or hash function to combine a symmetric key stored on device with a nonce to generate a one-time password. The cryptographic module performing this operation shall be validated at FIPS 140-2 Level 1 or higher." For single-factor and multi-factor cryptographic tokens at Assurance Level 2 or 3, NIST SP 800-63-1 requires: "The cryptographic module shall be validated at FIPS 140-2 Level 1 or higher."

DEA believes that NIST 800-63-1 Assurance Level 3 as described will meet its security concerns. As discussed above, DEA continues to believe that reliance on passwords alone, as a few commenters suggested, would not provide sufficient security in healthcare settings where computers are accessed and shared by staff. Many staff may be able to watch passwords being entered, and computers may be accessible to patients or other outsiders. In addition, DEA notes that practitioners might find strong passwords more burdensome than a biometric or token over the long run. Strong passwords generally need to be long (e.g., 8-12 characters) with a mix of characters, to maintain

security. They also need to be changed frequently (e.g., every 60 to 90 days). However, imposing these password requirements would make it more likely that practitioners would simply write down passwords, thereby rendering them useless for purposes of security. In contrast to the time limits typically required for strong passwords, a token and biometrics can last for years. Although initially simpler to implement, passwords impose a burden on the user, who has to remember and key in the password, and on the application, which has to reset passwords when the user forgets them. DEA is not allowing the use of some two-factor combinations. For example, look-up secret tokens or out-of-band tokens are not acceptable. Look-up secret tokens, which are something you have, are often printed on paper or plastic; the user is asked to provide a subset of characters printed on the card. Unlike a hard token, these tokens can be copied and used without the practitioner's knowledge, undermining non-repudiation. Out-of-band tokens send the user a message over a separate channel (e.g., to a cell phone); the message is then entered with the password. Although DEA recognizes that these tokens might work, DEA doubts if they are practical because they require more time for each authentication than the other options.

Based on the comments received, it appears that a number of commenters have already implemented a variety of hard tokens (e.g., proximity cards, USB devices) as an authentication credential to electronic applications. DEA is seeking information from commenters on their experiences implementing hard tokens as authentication credentials. DEA seeks the following information:

- Why was the decision made to adopt hard token(s) as an authentication credential? Why was the decision made to adopt hard tokens as opposed to another option? What other options were considered?
- What are hard token(s) as an authentication credential used for (e.g., access to a computer, access to particular records, such as patient records, or applications)?
- How many people in the practice/institution use hard tokens for authentication (number and percentage, type of employee – practitioners, nurses, office staff, etc.)?
- What types of hard tokens are used (e.g., proximity cards, USB drives, OTP devices, smart cards)?
- Are the hard tokens used by themselves or in combination with user IDs or passwords?
- How are the hard tokens read (where applicable), and what hardware is necessary (e.g., card readers built into keyboards, external readers attached to computers)?
- How are hard token readers distributed (e.g., at every computer workstation, at certain workstations based on location, allocated based on number of staff)?
- Was the adoption of hard tokens part of installation of a new system or an addition to existing applications?
- How long did the implementation process take? Was the time related to implementing hard tokens or other application installation issues?
- Which parts of the implementation were completed without difficulty?
- What challenges were encountered and how were they overcome?
- Were workflows affected during or after implementation and, if so, how were they affected and for how long?
- How do the users feel about the use of hard tokens as an authentication credential?
- Has the use of hard tokens as an authentication credential improved or slowed workflows? If so, how?
- Has the use of hard tokens as an authentication credential improved data and/or network security?

- What other benefits have been realized?

Comments. Practitioner organizations asked who will create and distribute hard tokens, and how losses, malfunctions, and application downtime will be handled. A physician stated that tokens should be able to create keys on the token immediately under user control to speed distribution and replacement that has been such a barrier in pilot work.

DEA Response. Who distributes the hard tokens will depend on the application being used. In some cases, the credential service provider, working in conjunction with the electronic prescription application provider, may distribute the hard tokens; in other cases, the credential service provider, working in conjunction with the electronic prescription application provider, may tell the practitioners what type of token is required (e.g., a smart card, thumb drive, PDA), then securely register or activate the token. DEA agrees with the commenter that the latter scenario would make replacement easier because the practitioner could purchase a new token locally and obtain a new credential without having to wait for the application provider to send a new token. DEA, however, believes it is better to provide flexibility and allow credential service providers, electronic prescription application providers, and practitioners to determine how to provide and replace tokens when they are lost or malfunction.

Electronic prescription application downtime is not specific to tokens; any electronic prescription application may experience downtime regardless of the authentication method used. Practitioners will always have the option of writing controlled substance prescriptions manually.

Comments. A physician stated that there are special problems for physicians in small practices who do not normally wear institutional identification badges and have tighter time and budget constraints than large organizations. He stated that consideration should be given to allowing some exemptions for small practices or physicians who are willing to accept some risk from less than ideal authentication such as the use of biometrics as a substitute for cryptographic two-factor authentication or use of private keys or other cryptographic secrets protected by software installed on computers in a limited controlled office environment that would allow operation with only the PIN from a defined set of computers that were shared in a small practice. The commenter asserted that the cost of cryptographic tokens is not large, but a potential barrier nonetheless.

DEA Response. As discussed above, DEA is allowing the use of biometrics as an alternative to hard tokens, as one factor in the two-factor authentication protocol. DEA disagrees, however, with allowing an exception from two-factor authentication for small practices. DEA recognizes the constraints on small practices, but believes that the interim final rule, which allows Level 3 tokens and biometrics, will make it easier for small practices. One-factor authentication, such as a PIN, will not provide adequate security, particularly in a small practice where passwords may be more easily guessed than in a large practice because the office staff will be familiar with the words a practitioner is most likely to use (e.g., nickname, favorite team, child's or pet's name).

Comments. A State agency reported on a vendor that uses a security matrix card; prescribers log on using a password and user ID and then have to respond to a challenge that corresponds to three interstices on the card. The commenter asserted that the challenge is unique to the provider, different every time, and only the card will provide

the correct response. The commenter asserted that although there are some vulnerabilities, it is simple and inexpensive.

DEA Response. DEA believes that such devices can be vulnerable as they may be physically reproduced and provided to others, or reproduced and used by others without the practitioner's knowledge. For that reason, DEA does not believe that these types of authentication tokens address DEA's concerns. Hard tokens are tangible, physical, objects, possessed by a practitioner. Giving this tangible, physical object to another person takes a specific physical act on the part of the practitioner. That act is difficult for the practitioner to deny, and thus strengthens the value of hard tokens as a method of security.

Comments. A pharmacy association and an application provider asked whether practitioners would need multiple tokens if they used multiple applications.

DEA Response. The number of tokens that a practitioner will need will depend on the applications and their requirements. It is possible that multiple authentication credentials could be stored on a single token (e.g., on a smart card or thumb drive). If a practitioner accesses two applications that require him to have a digital certificate, it is possible that a single digital certificate could be used for both.

D. Creating and Signing Electronic Controlled Substance Prescriptions

DEA proposed that controlled substance prescriptions must contain the same data elements required for paper prescriptions. DEA proposed that, as with paper prescriptions, practitioners or their agents would be able to create a prescription. When the prescription was complete, DEA proposed that the application require the practitioner to complete the two-factor authentication protocol. The application would then present at

least the DEA-required elements for review for each controlled substance prescription and the practitioner would have to positively indicate his approval of each prescription. Prior to signing, the proposed rule would have required the practitioner to indicate, with another keystroke, agreement with an attestation that he had reviewed the prescription information and understood that he was signing the prescription. The practitioner would then have signed the prescription for immediate transmission. If there was no activity for more than two minutes after two-factor authentication, the application would have been required to lock out the practitioner and require reauthentication to the signing function. The first intermediary that received the prescription would have been required to digitally sign and archive the prescription.

1. Reviewing prescriptions

DEA proposed that the application present to the practitioner certain prescription information including the patient's name and address, the drug name, strength, dosage form, quantity prescribed, directions for use, and the DEA registration number under which the prescription would be authorized. DEA further proposed to require the practitioner to indicate those prescriptions that were ready to be signed.

DEA proposed allowing practitioners to indicate that prescriptions for multiple patients were ready for signing and allow a single signing to cover all approved prescriptions.

Comments. A number of commenters were concerned about the data elements that must be presented to practitioners for review. Two application providers stated that the data elements should be limited because too much data will be confusing. They asserted that the patient's address is unlikely to be useful to practitioners as patients are

usually identified by name and date of birth; it is unlikely that most practitioners would recognize an address as incorrect. They also expressed their view that the practitioner did not need to see the DEA registration number associated with the prescription.

A practitioner organization expressed agreement with the requirement in the proposed rule that prior to the transmission of the electronic prescription, the application should show a summary of the prescription. It noted that while National Council for Prescription Drug Programs (NCPDP) SCRIPT provides fields and codes for all required data, not all are mandatory. In addition, this commenter indicated some applications do not show all of the DEA-required prescription information. The commenter asked how applications will be updated and/or modified to meet the specifications required in the proposed rule. Another commenter, an application provider, stated that developers will have to redesign the applications at the screen level and at the user permission level, which will add costs. An insurance organization stated that the current NCPDP standards do not accommodate the described process and will have to be revised to conform next generation electronic prescribing software to the DEA requirements. The commenter believed that this would create another delay in the eventual use of electronic prescribing for controlled substances.

DEA Response. DEA has revised the rule to limit the required data displayed for the practitioner on the screen where the practitioner signs the controlled substance prescription to the patient's name, drug information, refill/fill information, and the practitioner information. If there are multiple prescriptions for a particular patient, the practitioner information and the patient name could appear only once on the screen. The refill information, if applicable, will be a single number. For Schedule II substances, if a

practitioner is writing prescriptions indicating the earliest date on which a pharmacy may fill each prescription under § 1306.12(b), these dates will also have to appear, consistent with the current requirement for paper prescriptions. DEA emphasizes that although this rule allows for one element of the required controlled substance prescription information (the patient's address) not to appear on the review screen, the controlled substance prescription that is digitally signed by either the application or the practitioner and that is transmitted must include all of the information that has always been required under 21 CFR part 1306.

DEA realizes that many application providers will have to update their applications, but it notes that most perform regular updates and upgrades. They may choose to incorporate the changes required by these regulations as part of a regular revision cycle.

Comments. A few application providers objected to requiring a review of the prescription information by the practitioner prior to signing, stating that this is not required for paper prescriptions.

DEA Response. DEA recognizes that it is possible that some applications currently in use for the prescribing of noncontrolled substances might not require the practitioner to review prescription data prior to signing. Nonetheless, with respect to the prescribing of controlled substances, a practitioner has the same responsibility when issuing an electronic prescription as when issuing a paper prescription to ensure that the prescription conforms in all respects with the requirements of the CSA and DEA regulations. This responsibility applies with equal force regardless of whether the prescription information is entered by the practitioner himself or a member of his staff.

Whether the prescription for a controlled substance is on paper or in electronic format, it would be irresponsible for a practitioner to sign the prescription without carefully reviewing it, particularly where the prescription information has been entered by someone other than the practitioner. Careful review by the practitioner of the prescription information ensures that staff or the practitioner himself has entered the data correctly. Doing so is therefore in the interest of both the practitioner and patient. Electronic prescriptions are expected to reduce prescription errors that result from poor handwriting, but as reports by Rand Health have stated, the applications create the potential for new errors that result from keystroke mistakes.[18] Rand Health reported many electronic prescribing applications are designed to create a prescription using a series of drop down menus; some of the applications do not display the information after it is selected so that keystroke errors (e.g., selecting the wrong patient or drug) may be difficult to catch. Comments on the proposed rule from a State Pharmacy Board indicate that such keystroke errors do occur in electronic prescriptions. Recent research on electronic prescribing in the United States and Sweden also found that electronic prescriptions have problems with missing and incorrect information, which indicates that the applications allow prescriptions to be transmitted without information in the standard prescription fields.[19] A review screen should alert practitioners to these problems. DEA notes that a number of electronic prescription application providers indicated that their applications already meet this practitioner review requirement.

---

[18] Bell, D.S., et al., "A Conceptual Framework for Electronic Prescribing," J Am Med Inform Assoc. 2004; 11:60-70.

[19] Warholak, T.L. and M.T. Mudd. "Analysis of community chain pharmacists' interventions on electronic prescriptions." J. Am. Pharm. Assoc. 2009 Jan-Feb; 49(1): 59-64.
Astrand, B. et al. "Assessment of ePrescription Quality: an observational study at three mail-order pharmacies." BMC Med Inform Decis Mak. 2009 Jan 26; 9:8.

Comments. Practitioner organizations expressed the view that checking an "all" box should be sufficient if a practitioner approves all of the prescriptions displayed, as opposed to indicating each prescription approved individually. Two State agencies, an information technology organization, and application providers objected to DEA's proposal to allow signing of prescriptions for multiple patients at one time. Some commenters believed that allowing practitioners to sign prescriptions for multiple patients at one time posed health and safety risks for the patients. Others stated that the prescriber might not notice fraudulent prescriptions in a long list.

DEA Response. DEA agrees that allowing practitioners to simultaneously issue multiple prescriptions for multiple patients with a single signature increases the likelihood of the potential detrimental consequences listed by the commenters. Accordingly, DEA has revised the rule to allow signing of multiple prescriptions for only a single patient at one time. Each controlled substance prescription will have to be indicated as ready for signing, but a single two-factor authentication can then sign all prescriptions for a given patient that the practitioner has indicated as being ready to be signed. DEA notes that many patients who are prescribed controlled substances receive only one controlled substance prescription at a time.

2. Timing of authentication, lockout, and attestation

DEA proposed that the practitioner would use his two-factor authentication credential to access the review screen. The practitioner would indicate those prescriptions ready to be signed. Prior to signing, DEA proposed that the practitioner indicate agreement with the following statement: "I, the prescribing practitioner whose name and DEA registration number appear on the controlled substance prescription(s)

being transmitted, have reviewed all of the prescription information listed above and have confirmed that the information for each prescription is accurate. I further declare that by transmitting the prescription(s) information, I am indicating my intent to sign and legally authorize the prescription(s)." If there was no activity for two or more minutes, the application would have to lock him out; he would have to reauthenticate to the application before being able to continue reviewing or signing prescriptions.

Comments. DEA received a substantial number of comments on the timing of authentication and signing, lockout, and attestation. An application provider organization stated that delegating prescription-related tasks (e.g., adding pharmacy information) to practitioner staff is a vital step in the prescribing process. The commenter believed that requiring all such tasks to occur before the practitioner approves and signs the prescription would change the workflow in practitioners' offices. The application provider recommended that DEA allow for variable workflows in which ancillary information regarding the prescription, such as which destination pharmacy to send to, may be completed by the nurse after signing, but all other data specific to the medication dispensed be locked down and only editable by the prescribing practitioner. Another application provider suggested revising the requirement for reviewing and indicating that a prescription is ready to sign to read: "…where more than one prescription has been prepared at any one time[,]…prior to the time the practitioner authenticates to the application, the application must make it clear which prescriptions are to be signed and transmitted." This commenter expressed the view that although this may seem like a subtle distinction, the user interface design of electronic prescribing applications is variable, and many applications already clearly show the user which prescriptions are

awaiting signature and transmittal (for instance, by displaying them in a different frame on the screen or in a different color). The commenter asserted that a requirement that the user take further action to specify the prescriptions he/she will sign would be superfluous.

Commenters generally expressed concern about the additional keystrokes required to take these steps, stating that each new keystroke adds to the burden of creating an electronic prescription and discourages use of electronic prescriptions. An insurance organization stated that the process DEA proposed would require at least three practitioner confirmations of the electronic prescription. The commenter asserted that the more steps in the process, the less the workflow integration with current electronic prescribing workflow, and the increased potential for the reversion to written prescriptions. Another insurance organization stated the process of reviewing and signing should be streamlined. The commenter believed the process proposed by DEA seemed to have five steps with three confirmations.

Commenters were particularly concerned about the 2-minute lockout period. They were unsure whether it applied to the initial access to the application or to access to the signing function. A number of application providers stated that requiring two-factor authentication to sign the prescription would be more effective and eliminate the need for a lockout; that is, they advocated making the use of the two-factor authentication synonymous with signing a controlled substance prescription. One practitioner organization stated that the authentication and lockout could interrupt work flows; access to other functions of the electronic medical record must be available with the authentication. The application providers also noted that lockouts are easy to implement.

Those commenters who addressed the attestation statement expressed opposition to it. They emphasized that a practitioner must comply with the Controlled Substances Act and its implementing regulations in the prescribing of any controlled substance. Some were of the view that the statement did not serve any new purpose or address any new requirement. They emphasized that such a statement is not required for written prescriptions. Commenters further stated that they believed it would be an annoyance, and that practitioners would not read it, but would simply click it and move on. They also asserted that each additional step DEA added to the creation of an electronic prescription made it more likely that practitioners would decide to revert to paper prescriptions. Many individual practitioners indicated they found the statement unnecessary and demeaning. A few commenters stated that if DEA believed this was essential, it should be a one-time notice, similar to licensing agreements that appear on first use of a new application.

A number of organizations stated that they believed a better approach would be to present a simple dialog box with a clear and short warning that a prescription for a controlled substance is about to be signed. Some suggested this dialog could have three buttons: Agree, Cancel, and Check Record. Some commenters also noted that when prescribers get prescription renewal requests (for noncontrolled substances) in their electronic medical record applications now they have to minimize or temporarily "cancel" the request, check the chart for appropriateness, and then click yes or no. Commenters believed that the proposed rule does not seem to include this necessary capability.

DEA Response. DEA has revised the rule to limit the number of steps necessary to sign an electronic controlled substance prescription to two. Practitioners will not have to use two-factor authentication to access the list of prescriptions prior to signing. When they review prescriptions, they will have to indicate that each controlled substance prescription is ready for signing, then, as some commenters recommended, use their two-factor authentication credential to sign the prescriptions. If the information required by part 1306 is altered after the practitioner indicated the prescription was ready for signing, a second indication of readiness for signing will be required before the prescription can be signed.

As discussed previously, DEA has revised the rule to limit the required data displayed for the practitioner on the screen where the practitioner signs the controlled substance prescription to the patient's name, drug information, refill/fill information, and the practitioner information. The requirement in the proposed rule that the patient's address be displayed on the screen at this step of the process has been eliminated. (However, consistent with longstanding requirements for controlled substance prescriptions, the patient's address must be included in the prescription data transmitted to the pharmacy.) Because DEA is requiring that the application digitally sign the information required by the DEA regulations at the time the practitioner signs the prescription, additional non-DEA-required information (e.g., pharmacy URL) could also be added after signing. (See discussion below.) Using two-factor authentication as the signing function eliminates the need for the lockout requirement and, therefore, this rule contains no such requirement.

DEA has revised the rule to eliminate a separate keystroke for an attestation statement and adopted the suggestion of some of the commenters that the statement be included on the screen with the prescription review list. Further, DEA has revised the statement displayed. The statement will read: "By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above." The practitioner will not be required to take any action with regard to the statement. Rather, the statement is meant to be informative and thereby eliminate the possibility of any uncertainty as to the significance of completing the two-factor authentication protocol at that time and the limitation on who may do so. The only keystrokes that the practitioner will have to take will be to indicate approval of the prescription and affix a legal signature to the prescription by execution of the two-factor authentication protocol. DEA notes that some applications already present practitioners with a list of prescriptions ready to be signed and require their approval. For these applications, only the two-factor authentication will be a new step.

3. Indication that the prescription was signed

Because the National Council for Prescription Drug Programs SCRIPT standard does not currently contain a field for the signature of a prescription, DEA proposed that the prescription record transmitted to the pharmacy must include an indication that the practitioner signed the prescription. This indication could be a single character.

Comments. An application provider organization stated that existing logic in audit trails should cover the requirement for an indication that the prescription was signed. When a practitioner sends the prescription, the prescription is associated with the practitioner. One electronic prescription application provider objected to the addition of a field indicating that the prescription has been signed and asked whether the pharmacy could fill the prescription if the field was not completed. A standards development organization stated that DEA would have to request the addition of the field to NCPDP SCRIPT. Two application providers stated that without a prescription and signature format, there is no way to verify the signature.

DEA Response. DEA is not specifying by regulation how the field indicating that a prescription has been signed could be formatted, only that such a field must exist and that electronic prescription applications must indicate that the prescription has been signed using that particular field. As DEA noted in the NPRM, the field indicating that the prescription was signed could be a single character field that populates automatically when the practitioner "signs" the prescription. DEA is not requiring that a signature be transmitted. The field is needed to provide the pharmacy assurance that the practitioner in fact authorized the prescription. Although most existing applications may not transmit the prescription unless the prescription is approved or signed, and DEA is making that an application requirement, the pharmacy has no way to determine whether the electronic prescription application the practitioner used to write the prescription meets the requirement absent an indication that the prescription was signed. The prescription application's internal audit trail is not available to the pharmacist who has to determine whether he can legally dispense the medication. If a pharmacy receives an electronic

prescription for a controlled substance in which the field indicates that the prescription has not been signed, the pharmacy must treat this as it would any written prescription that does not contain a manual signature as required by DEA regulations.

The required contents for an electronic prescription for a controlled substance set forth in the interim final rule are the same contents that have long been required under the DEA regulations for all paper and oral prescriptions for controlled substances. As with all regulations issued by any agency, the DEA regulations are publicly available, every standards organization and application provider has access to them, and all persons subject to the regulations are legally obligated to abide by them. If any organization or application provider wants its standard or application to be compliant with the regulations and, therefore, usable for controlled substance prescriptions, they need only read the regulations and make any necessary changes.

Comments. A standards organization asked how the signature field affected nurses that act as agents for practitioners and nurses at LTCFs who are given oral prescription orders.

DEA Response. Longstanding DEA regulations allow agents of a practitioner to enter information on a prescription for a practitioner's manual signature and also permit practitioners to provide oral prescriptions to pharmacies for Schedule III, IV, and V controlled substances. Nurses, who are not DEA registrants, are not allowed to sign controlled substances prescriptions on behalf of practitioners regardless of whether the prescription is on paper or electronic. Accordingly, whether in the LTCF setting or otherwise, nurses may not be given access to, or use, the practitioner's two-factor authentication credential to sign electronic prescriptions for controlled substances.

4. Other prescription content issues

DEA proposed that only one DEA number should be associated with a controlled substance prescription.

Comments. A number of commenters associated with mid-level practitioners stated that some State laws require that a controlled substance prescription from a mid-level practitioner must contain the practitioner's supervisor's DEA registration number as well as the mid-level practitioner's DEA registration number. Other commenters noted that under § 1301.28 a DEA identification number is required in addition to the DEA registration number on prescriptions written by practitioners prescribing approved narcotic controlled substances in Schedules III, IV, or V for maintenance or detoxification treatment. Other commenters stated that the DEA requirements for paper prescriptions include, for practitioners prescribing under an institutional practitioner's registration, the special internal code assigned by the institutional practitioner under §§ 1301.22 and 1306.05. These commenters stated that NCPDP SCRIPT does not accommodate the special internal codes, which do not have a standard format, nor do most pharmacy computer applications. They also noted that a pharmacy has no way to validate the special internal codes.

DEA Response. DEA's concern with multiple DEA numbers on a single prescription is based on a need to be able to identify the prescribing practitioner. The interim final rule allows multiple DEA numbers to appear on a single prescription, if required by State law or regulations, provided that the electronic prescription application clearly identifies which practitioner is the prescriber and which is the supervisor. NCPDP SCRIPT already provides such differentiation.

DEA is aware of the issue of internal code numbers held by individual practitioners prescribing controlled substances as agents or employees of hospitals or other institutions under those institutions' registrations pursuant to § 1301.22(c). DEA published an Advance Notice of Proposed Rulemaking (74 FR 46396, September 9, 2009) to seek information that can be used to standardize these data and to require institutions to provide their lists of practitioners eligible to prescribe controlled substances under the registration of the hospital or other institution to pharmacies on request.

The problem with special codes for individual practitioners prescribing controlled substances using the institutional practitioner's registration and the DEA-issued identification number for certain substances used for detoxification and maintenance treatment is that SCRIPT does not currently have a code to identify them. Codes exist that identify DEA numbers and State authorization numbers; the fields are then defined to limit them to the acceptable number of characters. The general standard for the identification number field, however, is 35 characters. It should, therefore, be possible for NCPDP to add a code for an institution-based DEA number that allows up to 35 characters, with the first nine characters in the standard DEA format; the remaining characters should be sufficient to accommodate most institutional coding systems until DEA and the industry can standardize the format. Similarly, NCPDP should be able to add a code for the identification number for maintenance of detoxification treatment. Free text fields may also need to be used to incorporate other information required on certain prescriptions; for example, part 1306 requires that prescriptions for gamma hydroxybutyric acid the practitioner must indicate the medical need for the prescription;

for certain medications being used for maintenance or detoxification treatment, the practitioner must include an identification number in addition to his DEA number.

On the issue of the inability of pharmacies to validate the special code assigned by an institutional practitioner to individual practitioners permitted to prescribe controlled substances using the institution's DEA registration, DEA notes that the "validation" that some pharmacy applications conduct simply confirms that the DEA number is in the standard format and conforms to the formula used to generate the DEA registration numbers. The validation does not confirm that the number is associated with the prescriber listed on the prescription or that the registration is current and in good standing. To confirm the actual validity of the DEA number, the pharmacy would have to check the DEA registration database using the Registration Validation tool available at the Office of Diversion Control Web site (http://www.DEAdiversion.usdoj.gov). If a pharmacy has reason to question any prescription containing special identification codes for individual practitioners, it must contact the institutional practitioner.

DEA recognizes that revisions to the SCRIPT standard to accommodate identification codes for individual practitioners prescribing controlled substances using the institutional practitioner's registration, identification numbers for maintenance or detoxification treatment, and dates before which a Schedule II prescription may not be filled may not occur immediately as they have to be incorporated into a revision to the standard that is subject to the standards development process. Application providers will then have to incorporate the new codes into their applications.

Because DEA does not want to delay implementation of electronic prescribing of controlled substances for any longer than is necessary to accommodate the main

provisions of the rule, DEA has added provisions to §§ 1311.102 ("Practitioner responsibilities."), 1311.200 ("Pharmacy responsibilities."), and 1311.300 ("Third-party audits.") to address the short-term inability of applications to handle information such as this accurately and consistently. DEA is requiring that third-party auditors or certification organizations determine whether the application being tested can record, store, and transmit (for an electronic prescription application) or import, store, and display (for a pharmacy application) the basic information required under § 1306.05(a) for every controlled substance prescription, the indication that the prescription was signed, and the number of refills. Any application that cannot perform these functions must not be approved, certified, or used for controlled substance prescriptions. The third-party auditors or certification organizations must also determine whether the applications can perform these functions for the additional information required for a subset of prescriptions; currently this information includes the extension data, the special DEA identification number, the dates before which a prescription may not be filled, and notes required for certain prescriptions. If a third-party auditor or certification organization reports that an application cannot record, store, and transmit, or import, store, and display one or more of these data fields, the practitioner or pharmacy must not use the application to create, sign and transmit or accept and process electronic prescriptions for controlled substances that require this information.

Comments. Some commenters stated that the requirement that the prescription be dated would remove the ability to create several Schedule II prescriptions for future filling.

DEA Response. DEA does not allow practitioners to post-date paper prescriptions as some commenters seemed to think. Under § 1306.05(a), all prescriptions for controlled substances must be dated as of, and signed on, the day when issued. Under § 1306.12(b), practitioners are allowed to issue multiple prescriptions authorizing the patient to receive up to a 90-day supply of a Schedule II controlled substance provided, among other things, the practitioner indicates the earliest date on which a pharmacy may fill each prescription. These prescriptions must be dated on the day they are signed and marked to indicate the earliest date on which they may be filled. All of these requirements can (and must) be satisfied when a practitioner elects to issue multiple prescriptions for Schedule II controlled substances by means of electronic prescriptions. At present, it is not clear that the SCRIPT standard accommodates the inclusion of these dates or that pharmacy applications can accurately import the data. As noted in the previous response, until applications accurately and consistently record and import these data, applications must not be used to handle these prescriptions.

Comments. One application provider stated that DEA should not include the practitioner's name, address, and DEA number on the review screen because, in some cases, prescriptions are written for one of several practitioners in a practice to sign. This commenter stated that with paper prescriptions, there is no indication other than the signature as to which practitioner signed the prescription. A State pharmacist association asked DEA to require that the prescription include the practitioner's phone number and authorized schedules.

DEA Response. Only a practitioner who has issued the prescription to the patient for a legitimate medical purpose in the usual course of professional practice may sign a

prescription. As stated above, the requirements for the information on an electronic prescription are the same as those for a paper prescription. DEA notes that the NCPDP SCRIPT standard includes a field for telephone number, but DEA is not requiring its use. If a pharmacist has questions about a practitioner's registration and schedules, the pharmacist can check the registration through DEA's Web site.

Comments. One company recommended registering actual written signatures and associating them with electronic prescriptions. A State asked that digital ink signatures be recognized and be allowed on faxes; this would allow people to avoid using SureScripts/RxHub, which the commenter indicated is expensive.

DEA Response. DEA does not believe there is any way to allow the foregoing signature methods while providing an adequate level of assurance of non-repudiation. Verification of a manually written signature depends on more than the image of the signature.

5. Transmission on signing/Digitally signing the record

DEA proposed that the electronic prescription would have to be transmitted immediately upon signing. DEA proposed that the first recipient of the electronic prescription would have to digitally sign the record as received and archive the digitally signed copy. The digital signature would not be transmitted to the other intermediaries or the pharmacy.

Comments. Some commenters disagreed with the requirement that prescriptions be transmitted on signing. A practitioner organization and a health information technology group supported the requirement, but stated that DEA should word this so the intent is clear that the electronic prescription application is to be configured to

electronically transmit the prescription as soon as it has been signed by the prescriber. They stated that DEA must make it clear that an electronic prescription is not considered to be "transmitted" unless it has been successfully received by the pharmacist who will fill the prescription, and an acknowledgment has been returned to the prescriber's application. An application provider stated that DEA should remove the requirement for instant transmission of prescription data: Many electronic prescribing applications use processes where pending messages are stored and, with a fixed periodicity of 10 seconds, transmitted to electronic prescribing networks. The commenter believed that this requirement might require complete re-architecting of these processes, which would create a substantial burden on electronic prescribing application developers. A chain pharmacy stated that DEA should allow the prescriber the option to put the prescription in a queue or to immediately transmit. The commenter suggested that if opting to hold in a queue, the prescriber would have to approve prior to sending. If, however, the prescription is automatically held in a queue due to connectivity problems, the prescriber should not be required to re-approve the prescription.

A standards organization recommended extending to long-term care facilities (LTCFs) the option allowed to Federal health care agencies where the prescription may be digitally signed and "locked" after being signed by the practitioner, while allowing other facility-determined information, such as resident unit/room/bed, times of administration, and pharmacy routing information to be added prior to transmission. The commenter noted that these additional data elements are distinct from the prescription data required by § 1306.05(a). The commenter explained that this digitally signed version would be archived and available for audit. The organization stated that its

recommended process matches a key aspect of the accepted LTCF order workflow, where the nursing facility reviews each physician order in the context of the resident's full treatment regimen and adds related nursing and administration notes. The commenter explained that after review and nursing annotation, the prescription is forwarded to the appropriate LTC pharmacy. By requiring that the prescription be digitally signed immediately after the physician's signature (or upon receipt if the facility system is the first recipient of the electronic prescription), this rule could appropriately be extended to non-Federal nursing facilities, enabling them to meet existing regulations requiring review of resident medication orders by facility nursing staff prior to transmission to the pharmacy. A pharmacist organization, whose members work in LTCFs and similar facilities, stated that the rule may be impossible to put into operation without fundamental changes to pharmacy practice and workflow. Other commenters also stated that the workflow at LTCFs mean that nurses generally enter information about prescriptions into records and transmit them to pharmacies. The standards organization recommended a modification to allow nursing staff at LTCFs to review, but not change, the prescription before transmission. The commenter asserted that this modification would enable consultation with the prescriber regarding potential conflicts in the care of the resident, and could prevent dispensing of duplicate or unnecessary controlled medications. Further, the commenter asserted that this change would resolve a conflict between the proposed rule and existing nursing home regulations, which call for review of resident medication orders by facility nursing staff prior to their transmission to the pharmacy.

On the issue of having the first recipient digitally sign the DEA-required information, some commenters asked about the identity of the first recipient. One application provider expressed the view that unless the application provider is the first recipient, it cannot be held responsible for the digital signing and archiving. Where the first processor is a third-party aggregator, this commenter asserted, it should be responsible for complying. An application provider organization stated that adding a digital signature will greatly increase the storage cost of transaction data.

One application provider stated that if the prescription is created on an Internet-based application, such as one on which the prescriber uses an Internet browser to access the application, the prescription would actually be digitally signed on the Internet-based application provider's servers by the prescriber. Therefore, the initial digital signature archived on the Internet-based prescribing application would be that of the prescriber, created using the hardware cryptographic key, rather than that of the application provider. The commenter indicated that in this case, the application network provider, rather than the electronic prescription application provider, should digitally sign the prescription with its own digital signature and archive the digitally signed version of the prescription as received. The commenter asserted that for true ASP applications (web-based applications), the prescriber is actually digitally signing the prescription at the server. It is not necessary, this commenter indicated, for the web-based electronic prescription application provider to sign also. Some commenters thought that every intermediary would be required to digitally sign and archive a copy. A State board of pharmacy said the first recipient should not have to digitally sign the prescription unless the first

recipient is the pharmacy. The responsible pharmacist should have to digitally sign the prescription.

An application provider stated that the combination of authentication mechanisms, combined with reasonable security measures by the practice (e.g., at a minimum, not sharing or writing down passwords), is sufficient to prevent abuse. Additionally, this commenter indicated, the audit logs should be sufficient to recognize and document fraud or forgery. The commenter stated that the requirement for digitally signing the record should be dropped.

DEA Response. DEA has revised the rule to eliminate the need for signing and transmission to occur at the same time. Under the proposed rule, the application of the digital signature to the information required under part 1306 would have occurred after transmission. Hence, under the proposed rule, it was critical that the information be transmitted immediately so that the DEA-required information could not be altered after signature but before transmission. Under the interim final rule, however, the application will apply a digital signature to and archive the controlled substance prescription information required under part 1306 when the practitioner completes the two-factor authentication protocol. Alternatively, the practitioner may sign the controlled substance prescription with his own private key. Because of the digital signature at the time of signing, the timing of transmission is less critical. DEA expects that most prescriptions will be transmitted as soon as possible after signing, but recognizes that practitioners may prefer to sign prescriptions before office staff add pharmacy or insurance information. In long-term care facilities, nurses may need to transfer information to their records before transmitting. By having the application digitally sign and archive at the point of two-

factor authentication, practitioners and applications will have more flexibility in issuing and transmitting electronic prescriptions.

DEA does not believe that the security mechanisms that the application provider cited at a practitioner's office would sufficiently provide for non-repudiation. DEA disagrees with the State Board of Pharmacy that the first recipient or the electronic prescription application need not digitally sign the record. Unless the record is digitally signed before it moves through the transmission system, practitioners would be able to repudiate prescriptions by claiming that they had been altered during transmission (inadvertently or purposefully). The only way to prove otherwise would be to obtain (by subpoena or otherwise) all of the audit log trails from the intermediaries, assuming that they retained them. As DEA is not requiring the intermediaries to retain records or audit trails, it might not be possible to obtain them. In addition, unless a practitioner was transmitting prescriptions to a single pharmacy, the number of intermediaries involved could be substantial; although the practitioner's application might use the same routers to reach SureScripts/RxHub or its equivalent, each of the recipient pharmacies may rely on different intermediaries.

6. PKI and Digital Signatures

DEA proposed an alternative approach, limited to Federal healthcare facilities, that would be based on public key infrastructure (PKI) and digital signature technology. Under this approach, practitioners would obtain a digital certificate from a certification authority (CA) cross-certified with the Federal Bridge CA (FBCA) and use the associated private key to digitally sign prescriptions for controlled substances. DEA proposed this approach based on requests from Federal health care agencies that have implemented PKI

systems. Those agencies noted that the option DEA proposed for all health care practitioners did not meet the security needs of Federal health care agencies.

Comments. A number of commenters, including practitioner associations, one large chain drug store, several electronic prescription application providers, and organizations representing computer security interests asked DEA to allow any practitioner or provider to use the digital signature approach, as an option. A pharmacist organization and a standards development organization stated that long-term care facilities should be able to use this approach. A practitioner organization and a healthcare management organization stated that the system would be more secure, and prescribers' liability would be reduced, if prescribers could digitally sign prescriptions. Three application providers preferred applying a practitioner's digital signature rather than a provider's. They stated that the added burden to the electronic health record is authentication using smart-cards (of a well known format), and that it can wrap the NCPDP SCRIPT prescription in XML-Digital signature envelop with a signature using the identity of the authenticated user. The commenters stated that the added burden to the healthcare provider is the issuance of a digital certificate that chains to the Federal PKI, possibly SAFE Biopharma or possibly extending the Federal PIV card. A State pharmacist organization asked why DEA is in favor of a system that is less secure than the one Federal health agencies use.

Some commenters noted that although the current system, based on intermediaries, makes use of digital signatures difficult, changes in technology may make it feasible in the future. In addition, for healthcare systems with their own pharmacies, a PKI-based approach would be feasible now. An intermediary stated that NCPDP

SCRIPT could not accommodate a digital signature, but other IT organizations argued that this is not necessarily true. One information technology security firm stated that companion standards to NCPDP SCRIPT standard in XML and HL7, which ought to be considered, include the W3C's XML digital signature standard (XML-DSig) and the Document Digital Signature (DSG) Profile. Several application providers stated:

> The prescription should be digitally signed using encapsulated XML Digital Signature with XADES profile. The specific profile is recognized for optional use by CCHIT [the Certification Commission for Healthcare Information Technology] in S28. This is fully specified in HITSP C26 for documents, which points at the IHE DSG profile. HITSP C26 and IHE DSG profile uses detached signatures on managed documents. This might be preferred as it would have the least impact on the existing data flow, or further profiling could support encapsulation if necessary. CCHIT S28 is not fully clear and has not yet been tested.

An information technology organization stated that DEA should require PKI. The government has a highly secure, interoperable digital identity system for Federal agencies and cross-certified entities through FBCA. The commenter asserted that this system should provide the framework for DEA's rule for electronic prescribing of controlled substances. The commenter believed that it is a widely available and supported system that provides the level of security, non-repudiability, interoperability, and auditability required by legislation covering the prescribing of controlled substances. The commenter stated that such a system would provide strong evidence that the original prescription was signed by a DEA-registered practitioner, that it was not altered after it was signed and transmitted, and that it was not altered after receipt by the pharmacist.

An information technology provider suggested the application allow the end users to choose credential types, including PKI and/or One Time Password (OTP) credentials, and recommended end users be permitted to use their existing PKI credentials if their

digital certificates met Federal Medium Assurance requirements and are issued from a CA that is cross-certified with the Federal Bridge. The commenter asserted that it is expected that there will be a number of service providers who will offer a turnkey PKI service to issue digital certificates for non-Federal entities that meet these requirements. This would lower costs for the overall system and would foster a stronger adoption curve for end users because they may be able to use a device they already possess to secure online accounts.

A PKI system designer noted that digital signatures can be used for any data. Once prescription and pharmacy applications are using the same version of SCRIPT the commenter believed there will be no need for conversion of prescriptions from one software version to another. The commenter further asserted that:

> … prescriptions need not be sent in a format that can be immediately interpreted by a pharmacy computer. It would be efficient, but it is not necessary. Free text messages can be digitally signed, too. …Free text messages may not be as efficient as NCPDP SCRIPT messages, but they do the job, just as the scores of faxes or paper-based prescriptions do, only better and faster.

Another information technology firm noted that digital signatures work for systems as simple as email and PDF. The commenter stated that Adobe Acrobat is capable of performing signature validation and checking for certificate revocation using either a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) request.

An intermediary further stated that the FIPS 186-2 Digital Signature Standard published in January 2000 has some shortcomings that are addressed in the current draft version FIPS 186-3 of the standard. The commenter believed these shortcomings relate to the signature schemas. The commenter asserted that FIPS 186-2 does not support RSA

signature schemes according to Public Key Cryptography Standard (PKCS) #1 version 2.1, which is a widely used industry standard. The commenter indicated that PKCS#1 is added to the FIPS 186-3 draft for the Digital Signature Standard. Therefore, the commenter asserted, signatures according to PKCS#1 version 2.1 (RSASSA-PKCS1-v1_5 and RSASSA-PSS) should also be considered as appropriate for electronic prescriptions for controlled substances. This same commenter asserted that the minimum key sizes for digital signatures should meet the requirements specified in NIST SP 800-57 Part1.

DEA Response. DEA agrees with the practitioner organizations and other commenters that the digital signature option should be available to any practitioner or group that wants to adopt it and has revised the interim final rule to provide this option to any group. DEA believes it is important to provide as much flexibility as possible in the regulation and accommodate alternative approaches even if they are unlikely to be widely used in the short-term. DEA notes that a number of commenters, including a major pharmacy chain, anticipate that once the SCRIPT standard is mature, the intermediaries will no longer be needed and prescriptions will then move directly from practitioner to pharmacy as they do in closed systems. At that point, the PKI/digital signature approach may be more efficient and provide security benefits. In the short-term, some closed systems may find this approach advantageous. DEA emphasizes that the use of a practitioner digital signature is optional. DEA is including the option to accommodate the requirements of existing Federal systems and to provide flexibility for other systems to adopt the approach in the future if they decide that it would provide benefits for them.

Under the interim final rule, using a private key to sign controlled substance prescriptions will be an option provided that the associated digital certificate is obtained from a certification authority that is cross-certified with the Federal PKI Policy Authority at a basic assurance level or above. The electronic prescription application will have to support the use of digital signatures, applying the same criteria as proposed for Federal systems. The private key associated with the digital certificate will have to be stored on a hard token (separate from the computer being accessed) that meets the requirements for FIPS 140-2 Security Level 1 or higher. If a practitioner digitally signs a prescription with his own private key and transmits the prescription with the digital signature attached, the pharmacy will have to validate the prescription, but no other digital signatures will need to be applied. (If the practitioner uses his own private key to sign a prescription, the electronic prescribing application will not have to apply an application digital signature.) If the digital signature is not transmitted, the pharmacy or last intermediary will have to digitally sign the prescription. DEA emphasizes that Federal systems will be free to impose more stringent requirements on their users, as they have indicated that they do.

As noted in other parts of this rulemaking, DEA has updated the incorporation by reference to FIPS 186-3, June 2009.

E. Internal Audit Trails

DEA proposed that an application provider must audit its records and applications daily to identify if any security incidents had occurred and report such incidents to DEA.

Comments. One application provider stated that daily audit log checks would not be feasible and objected to reporting incidents as no parallel requirement exists for paper

prescriptions. The application provider stated that SureScripts/RxHub transmission standards should address all security concerns.

DEA Response. DEA disagrees with this commenter. At the July 2006 public hearing,[20] application providers stated that their applications had internal audit trails and they suggested that the audit function provided security and documentation. In the HIMSS 2009 Security Survey 83 percent of respondents reported having audit logs for access to patient records. The requirement for an internal audit trail should, therefore, not impose any additional burden on most application providers. DEA is requiring the application provider to define auditable events and run a daily check for such events. DEA does not expect that many such auditable events should occur. When they do occur, the application must generate a report for the practitioner, who must determine whether the event represented a security problem. DEA notes that only one application provider who commented on the NPRM had concerns regarding this requirement. The SureScripts/RxHub transmission standards provide no protection for attempts to access a practitioner's application.

Although practitioners are not expressly required under the DEA regulations to report suspected diversion of controlled substances to DEA, all DEA registrants have a duty to provide effective controls and procedures to guard against theft and diversion of controlled substances.[21] Accordingly, there is a certain level of responsibility that comes with holding a DEA registration. With that responsibility comes an expectation of due

[20] Transcripts, written comments, and other information regarding DEA's public meeting to discuss electronic prescriptions for controlled substances, held in conjunction with the Department of Health and Human Services, may be found at http://www.DEAdiversion.usdoj.gov/ecomm/e_rx/mtgs/july2006/index.html

[21] 21 CFR 1301.71(a).

diligence on the part of the practitioner to ensure that information regarding potential diversion is provided to law enforcement authorities, where circumstances so warrant. This requirement is no less applicable in the electronic prescribing context than in the paper or oral prescribing context. In fact, this concern might be heightened in the electronic context, due to the potential for large-scale diversion of controlled substances that might occur when a practitioner's electronic prescribing authority has fallen into unauthorized hands or is otherwise being used inappropriately.

Comments. An application provider organization and two application providers asked how security incidents should be reported. A healthcare system had concerns about reporting an incident before it could be investigated. Another healthcare system requested further clarification and detail surrounding the documentation requirements for findings and reporting of suspicious activity. A number of commenters recommended differing reporting periods from the end of the business day to 72 hours.

DEA Response. At this time, DEA is not specifying by rule how a security incident should be reported. Accordingly, practitioners have several options, including providing the information to DEA by telephone or email. If DEA finds over time that enough of these reports are being submitted to merit a standard format, DEA may develop a reporting form in the future. As DEA and registrants gain experience with these incidents, DEA will be able to provide guidance on the specific information that must be included in the reports. In general, the security incidents that should be reported are those that represent successful attacks on the application or other incidents in which someone gains unauthorized access. These should be reported to both DEA and the

application provider because a successful attack may indicate a problem with the application.

DEA recognizes the concern about reporting incidents before the practitioner or application provider has had a chance to investigate. DEA's experience with theft and loss reporting, however, indicates that waiting for investigation may delay reporting for long periods and make it difficult to collect evidence. DEA believes that one business day is sufficient. DEA notes that this is the same length of time required under the regulations for reporting of thefts or significant losses of controlled substances.[22]

F. Recordkeeping, Monthly Logs

1. Recordkeeping

DEA proposed that all records related to controlled substance electronic prescriptions be maintained for five years. DEA also proposed that the electronic records must be easily readable or easily rendered into a format that a person can read.

Comments. Pharmacy commenters generally objected to the five-year record retention requirement, noting that they are required to retain paper prescriptions for only two years. Commenters believed that the added retention time conflicted with many State pharmacy laws and regulations. They also believed there would be additional costs for purchase of added storage capacity. Some electronic prescription application providers expressed their view that 21 U.S.C. 827 limits the applicability of DEA recordkeeping requirements solely to registrants. Accordingly, they believed that DEA has no statutory authority to impose recordkeeping requirements on application providers or intermediaries. Some of the commenters also stated they believed that 21 U.S.C.

[22] 21 CFR 1301.76(b).

827(b) does not give DEA statutory authority to require registrants to maintain records for more than two years. Finally, with respect to the statutory recordkeeping requirements for practitioners, some commenters stated they believed that the recordkeeping provisions are limited to the two sets of circumstances set forth at 21 U.S.C. 827(c)(1)(A) and (B). They stated that if they were required to electronically store other data, such as that relating to identity proofing and transmissions with the digital signature and the monthly reports, this would result in overhead costs that application providers might not find relevant to the delivery of patient care and thus spending time developing such databases would have no value to the delivery of patient care. Commenters noted that these requirements are not part of the paper process and questioned why DEA would introduce it here. Commenters indicated that if five years of transactional data must be stored electronically for immediate retrieval, the cost to the application provider will be prohibitive. If offline or slower means of data storage retrieval are required, the cost to the application provider will be drastically reduced while still providing data to the Administration in a timely manner. Finally, a State health care agency asked that all records handled by intermediaries should be easily sorted, should provide a clear audit trail, and should be available to law enforcement.

DEA Response. In response to the comments, DEA has in the interim final rule changed the record retention period from that set forth in the proposed rule to two years, which is parallel to the requirement for paper prescriptions. Although DEA has revised the requirement, it should be noted that if the State in which the activity occurs requires a longer retention period, the State law must be complied with in addition to, and not in lieu of, the requirements of the Controlled Substances Act.

With respect to the issue of placing certain recordkeeping responsibilities on application providers, which are nonregistrants, the following considerations should be noted. While the express recordkeeping requirements of the CSA (set forth in 21 U.S.C. 827) apply only to registrants, DEA has authority under the Act to promulgate "any rules, regulations, and procedures [that the agency] may deem necessary and appropriate for the efficient execution of [the Act]." (21 U.S.C. 871(b)). DEA also has authority under the Act "to promulgate rules and regulations * * * relating to the * * * control of the * * * dispensing of controlled substances." (21 U.S.C. 821). The requirements set forth in the interim final rule relating to recordkeeping by nonregistrant application providers are being issued pursuant to this statutory authority. As stated in the interim final rule, for the purpose of electronic prescribing of controlled substances, DEA registrants may only use those applications that comply fully with the requirements of the interim final rule.

It should also be noted that DEA is not requiring practitioners to create a copy of a prescription or a new record; it is requiring the practitioner to use an application that stores a copy of the digitally signed record and retains the record for two years. These records will be stored on an application service provider's servers if the practitioner is using an application service provider to prescribe or on the practitioner's computers for installed applications. DEA further notes that the electronic prescribing of controlled substances is voluntary; no practitioner is required to issue controlled substance prescriptions electronically.

Although DEA had proposed having the first intermediary store the record, after taking into consideration the comments received to the NPRM, DEA decided that this approach risked losing the records. The practitioner can determine, through audit or

certification reports, whether an electronic prescribing application meets DEA's requirements, but it may be difficult for the prescribing practitioner to ensure that an intermediary meets DEA's requirements if the first intermediary is a different firm, as it often is. Intermediaries may change or go out of business, destroying any records stored; intermediaries may also subcontract out some of the functions, further attenuating controls.

2. Monthly logs

DEA proposed that the electronic prescription application would have to generate, on a monthly basis, a log of all controlled substance prescriptions issued by a practitioner and provide the log to the practitioner for his review. DEA further proposed that the practitioner would be required to review the log, but would not be expected to cross-check it with other records. As DEA explained in the NPRM, the purpose of the log review was to provide a chance for the practitioner to spot obvious anomalies, such as prescriptions for patients he did not see, for controlled substances he did not prescribe, unusual numbers of prescriptions, or high quantity of drugs. The practitioner would have to indicate that he had reviewed the log.

Comments. Commenters were divided on the viability and necessity of the log provision. Several practitioner organizations and one application provider stated that logs should be available for review, but opposed the requirement that practitioners confirm the monthly logs. A long-term care facility organization stated the log would be useful for detecting increased prescribing patterns. It, however, said the brief review proposed was too short and that the review should be reimbursable under Medicare. Other commenters stated that without checking the patients' records, it is unclear how this would increase

the likelihood of identifying diversion. The State agency said the rule did not definitively state the mechanism for the review. A healthcare system stated that it would be helpful if DEA would provide further clarification surrounding the type of information that would need to be maintained. This commenter further asserted that DEA should allow noncontrolled prescription drug activity to be reviewed and archived in the same manner so as not to duplicate work for the physician.

Other practitioner groups and application providers opposed the requirement that the practitioner review the monthly log check because such review is not required for paper prescriptions and because, these commenters asserted, it would be difficult to do without cross-checking patient records. An application provider stated that DEA does not have the authority to require the monthly log as 21 U.S.C. 827(c)(1) exempts practitioners from keeping prescription records. Some commenters mistakenly assumed that pharmacies would be generating the logs and that practitioners would have to review multiple logs each month; they opposed the requirement on that basis. An application provider and a State agency expressed doubt about the benefits of the requirement given the number of prescriptions that might be in an individual practitioner's monthly log. A few commenters suggested that DEA should enhance the log requirement to require the electronic prescription application to generate the logs every week (rather than every month, as was proposed). One application provider said that any log requirement would discourage electronic prescribing. Several commenters stated that the check would not enhance non-repudiation. A practitioner organization and a practitioner said that many providers would be worried about their liability if they fail to detect fraud. These commenters suggested that the regulations should protect unintentional failure to detect

fraud and the purpose of the logs should be exclusively to help physicians recognize fraud if they are able to do so, but without penalty for failures to catch errors if a good faith review and signature were performed. Another practitioner organization stated that DEA did not detail the practitioner's ultimate responsibility to review and approve the information in the logs, the manner and timeframe in which the review must be completed, or the practitioner's liability for failing to review the log. The commenter asserted that this obligation, as well as the other requirements, seems to create a new practice standard that places more responsibility, and thus increased liability, for proper implementation of the law on practitioners. In addition, this commenter expressed the view that there is a need to specify the confidentiality of all such records, including who has access and under what circumstances.

A State board of pharmacy said that a review of prescription monitoring records should be accepted as a substitute. Several commenters asked that the review be done electronically. A State agency stated that DEA should prohibit the practitioner from delegating the review to members of his staff.

DEA Response. DEA continues to believe that the monthly log requirement serves an important function in preventing diversion of controlled substances. In view of the comments, however, DEA has modified the requirement to lessen the burden on practitioners. Specifically, under the interim final rule, as in the proposed rule, the electronic prescription application will be required to generate, on a monthly basis, a log of all controlled substance prescriptions issued by a practitioner and automatically provide the log to the practitioner for his review. However, DEA has eliminated from the interim final rule the requirement that the practitioner mandatorily review each of the

monthly logs. DEA believes this strikes a fair balance in the following respects. Maintaining in the rule the requirement that the application supply the practitioner with the monthly log will ensure that all practitioners receive the logs on a regular basis without requiring practitioners to expend extra time and effort to request the logs. As a practical matter, this will result in more practitioners actually receiving the logs and, in all likelihood, more practitioners actually reviewing logs than would be the case if practitioners had to affirmatively request each time that the application send the log. The more practitioners review the logs, the more likely it will be that they will detect, without excessive delay, any instances of fraud or misappropriation of their two-factor authentication credentials. Such early detection will allow for earlier reporting by the practitioner of these transgressions and thereby more quickly cut off the unauthorized user's access to electronic prescribing of controlled substances. Ultimately, this is likely to result in fewer instances of diversion of controlled substances and less resulting harm to the public health and safety.

DEA is also maintaining in the interim final rule the requirement that the application be able to generate a log, upon request by the practitioner, of all electronic prescriptions f*or controlled substances the practitioner issued using the application over at least the preceding two years. As was proposed, the interim final rule requires that this log, as well as the monthly logs, be sortable at least by patient name, drug name, and date of issuance.

With respect to 21 U.S.C. 827, it is true that this provision sets forth the statutorily mandated recordkeeping requirements for DEA registrants. However, this provision does not preclude DEA from requiring that practitioners who elect to prescribe

controlled substances electronically use applications that meet certain standards designed to reduce the likelihood of diversion. In this same vein, nothing in 21 U.S.C. 827 precludes DEA from requiring that practitioners, when electronically prescribing controlled substances, use applications that, among other things, maintain records that the agency reasonably concludes are necessary to ensure proper accountability. As stated at the outset of this preamble, DEA has broad statutory authority to promulgate any rules and regulations that the agency deems necessary and appropriate to control against diversion of control substances or to otherwise efficiently execute the agency's functions under the CSA.[23]

G. Transmission Issues

DEA proposed that the information required under part 1306 including the full name and address of the patient, drug name, strength, dosage form, quantity prescribed, directions for use, and the name, address, and registration number of the practitioner must not be altered during transmission; it could be reformatted.

1. Alteration during transmission

Comments. Many commenters misinterpreted this requirement to mean pharmacies would not be able to substitute generic versions for brand name versions as is allowed under many State laws. One application provider organization suggested that the rule state that no changes are allowed on the medication segment and an application provider could only augment the segments of the prescription pertaining to transaction, transaction source, patient, or physician. Further, this commenter suggested, the

[23] 21 U.S.C. 821, 871(b).

application provider would not be able to edit any existing data. A healthcare organization asked how alteration of content is identified (e.g., according to FIPS 180-2).

DEA Response. DEA has revised the rule to clarify that the content of the required information must not be altered "during transmission between the practitioner and pharmacy." The requirement not to alter prescription information during transmission applies to actions by intermediaries. It does not apply to changes that occur after receipt at the pharmacy. Changes made by the pharmacy are governed by the same laws and regulations that apply to paper prescriptions. Again, any applicable State laws must also be complied with. As for changes by intermediaries during transmission, DEA is limiting only changes to the DEA-required elements (those set forth in 21 CFR part 1306). An intermediary could add information about the practitioner other than his name, address, and DEA registration number or about the patient, other than name and address. Alteration during transmission would be identified by comparing the digitally signed prescription retained by the electronic prescription application and the digitally signed prescription retained by the pharmacy.

2. Printing after transmission and transmitting after printing

DEA proposed that if a prescription is transmitted electronically, it could not be printed. If it was printed, it could not be transmitted electronically.

Comments. A number of commenters raised issues related to this requirement. A standards development organization noted that in some cases electronic prescriptions may be cancelled, for example when a transmission fails. In such cases, the commenter believed retransmission should be allowed. Pharmacies and pharmacy organizations stated that if transmission fails, the practitioner should be able to print the prescription.

Practitioner organizations suggested the following language: "If electronic transmission is prevented by weather, power loss, or equipment failure, or other similar system failure, prescriptions may be faxed to the pharmacy or printed." A healthcare organization stated that the rule does not define processes for transmission failures. The commenter asked if a second prescription is issued because the first was not received, how it would be clear that the first was cancelled. Many commenters, including pharmacy organizations, practitioner organizations, and electronic prescription application providers, stated that DEA should allow printing of a copy of the electronically transmitted prescription if it is clearly labeled as a copy. They noted that copies are often needed for insurance files and medical records; patients may be given a receipt listing all prescriptions written. Long-term care organizations also stated that these printed prescriptions were necessary for medication administration records.

DEA Response. DEA had noted in the preamble of the NPRM that transmitted prescriptions could be printed for medical records and other similar needs. DEA agrees with the commenters that such a statement should appear in the regulatory text and has revised the interim final rule to allow printing of a copy of a transmitted prescription, receipt, or other record, provided that the copy is clearly labeled as a copy that is not valid for dispensing. The copy should state, as recommended by commenters, that the original prescription was sent to [pharmacy name] on [date/time] and that the copy may not be used for dispensing. Printed copies of transmitted prescriptions may not be signed.

DEA has also added a provision that the application may print a prescription for signing and dispensing if transmission fails. DEA will require that these original prescriptions include a note to the pharmacy that the prescription was originally

transmitted to a specific pharmacy, but that the transmission failed. DEA considers this warning necessary because it is possible that the practitioner will be notified of a failure while the application is still attempting to transmit the prescription. The warning will alert the pharmacy to check its records to be certain a later transmission attempt had not succeeded. If the printed prescription is to be used for dispensing, it must be manually signed by the prescribing practitioner pursuant to § 1306.05(a). As the printed prescription contains information regarding the prior transmission, this information will be retained by the pharmacy.

Comments. A commenter recommended retaining the proposed language, but allowing the use of the SCRIPT CANCEL transaction. The commenter believed this would allow the application to either print the prescription or transmit it to another pharmacy. It noted that most vendors have not implemented support of this transaction. The commenter recommended that intermediaries that certify electronic prescription applications and pharmacy applications for interoperability should have to test and verify that vendors support the message before they are certified to accept controlled substances prescriptions.

DEA Response. DEA agrees that if a transmission fails or is canceled, the practitioner will be able to print the prescription or transmit it to another pharmacy. DEA, however, does not believe it is appropriate to attempt through these regulations to dictate to intermediaries that certify electronic prescription applications and pharmacy applications for interoperability what to cover in their certification requirements. DEA does not consider it advisable to include, as part of its regulations, references to particular

functions in the SCRIPT standard, or any other standard, as these standards are constantly evolving.

Comments. A healthcare organization suggested a requirement for the receiving pharmacy to provide confirmation back to the prescriber's application. The commenter suggested that the confirmation may then be printed and given to the patient, thereby providing documentation to demonstrate that the patient's prescription has been successfully transmitted to the patient's pharmacy.

DEA Response. Based on the comments, DEA does not believe that a requirement for a return receipt that would be provided to the patient would be reasonable because it would reduce the flexibility of the system. It would force the practitioner to write and transmit the prescription while the patient was still in the office. DEA does not have a similar requirement for oral or facsimile transmissions of paper Schedule III, IV, and V prescriptions and does not believe that this is warranted or necessary. In addition, as commenters made clear, it is not always possible to access a transmission system at a particular point in time.

3. Facsimile transmission of prescriptions by intermediaries

DEA proposed that intermediaries could not convert an electronic prescription into a fax if transmission failed. They would be required to notify the practitioner, who would then have to print and manually sign the prescription.

Comments. A standards development organization, several electronic prescription application providers, and a pharmacy chain stated that intermediaries should be able to convert electronic prescriptions to faxes if the intermediaries cannot complete the transmission. One electronic prescription application provider stated that 20 percent

of its transmissions need to be converted to facsimile because of pharmacy technology problems. An application provider organization stated that DEA is requiring that the prescription be digitally signed, so the prescription would have been signed. In the case of a temporary communication outage between physician and pharmacy, the commenter suggested that the pharmacy could receive a fax containing the ID tags of the script message. Those ID tags could then be later confirmed against the SCRIPT transaction when connectivity is resumed. The commenter believed that if DEA does not allow faxing by the intermediary, a unique workflow will be necessary for controlled substance transaction errors not required for legend drugs.

One State Board of Pharmacy stated that it had found many problems with electronic prescriptions. Among the problems this State Board reported was that even when pharmacies are able to receive electronic prescriptions, their applications do not necessarily read electronic prescriptions accurately. Data entered by a practitioner may be truncated in the pharmacy application or moved to another field. These statements were echoed by a State pharmacist association.

One application provider asked if faxed electronic prescriptions can continue to be treated as oral prescriptions.

DEA Response. A faxed prescription is a paper prescription and, therefore, must be manually signed by the prescribing practitioner registered with DEA to prescribe controlled substances. If an intermediary cannot complete a transmission of a controlled substance prescription, it must notify the practitioner in the manner discussed above. Under such circumstances, if the prescription is for a Schedule III, IV, or V controlled substance, the practitioner can print the prescription, manually sign it, and fax the

prescription directly to the pharmacy. DEA recognizes that not all pharmacies are currently capable of receiving fully electronic prescriptions and that there may be other transmission issues; however, it would be incompatible with effective controls against diversion to allow unsigned faxes of controlled substance prescriptions to be generated by intermediaries. As the commenters indicated, most of the reported transmission problems have to do with the lack of a mature standard for electronic prescriptions and the number of pharmacies that are not accepting electronic prescriptions. A number of commenters indicated that they anticipate that the need for intermediaries will disappear once the standard is mature. At that point, the issue of faxes will also be eliminated. As for the comment about treating faxed electronic prescriptions as oral prescriptions, this practice is not allowed under DEA's regulations as the commenter seemed to believe. To reiterate, the regulations have always required that a facsimile of a Schedule III, IV, or V prescription be manually signed by the prescribing practitioner.

Comments. A State Board of Pharmacy and a healthcare organization stated that under New Mexico and California law it was permissible to electronically generate a prescription and fax it. One commenter indicated that New Mexico allows electronic prescriptions to be sent "by electronic means including, but not limited to, telephone, fax machine, routers, computer, computer modem or any other electronic device or authorized means." A commenter noted that California, among others, allows for the faxing of controlled substances prescriptions with the text "electronically signed by" on the fax.

DEA Response. As discussed above, under DEA's regulations, a faxed prescription is a paper prescription and must be manually signed. It is not permissible to

electronically generate and fax a controlled substance prescription without the practitioner manually signing it.

4. Other Issues

Comments. Several electronic prescription application providers stated that DEA had not specified the characteristics of the transmission system between the practitioner and the pharmacy, which could be insecure. They recommended that a clear "secured" communication be used between the electronic prescription application and the pharmacy. Commenters recommended that the communications should meet HITSP T17 "Secured Communications Channel" requirements. They stated that this is already required, though not tested, by the Certification Commission for Healthcare Information Technology today (S28, S29). One State agency recommended requiring end-to-end encryption. An electronic prescription and pharmacy application provider and an intermediary described their network security. A practitioner organization stated that DEA should not over-specify requirements because other specifications exist with which DEA's requirements must coexist.

DEA Response. DEA has not addressed the security of the transmission systems used to transmit electronic prescriptions from practitioners to pharmacies, although some commenters asked DEA to do so and others claimed that the security of these systems provided sufficient protection against misuse of electronic prescriptions. As noted previously, the existing transmission system routes prescriptions through three to five intermediaries between a practitioner and the dispensing pharmacy. Practitioners and pharmacies have no way to determine which intermediaries will be used and, therefore, no way to avoid intermediaries that do not employ good security practices. As a practical

matter, once a practitioner purchases an electronic prescription application, the practitioner must accept whatever transmission routing the application provider employs. Neither the practitioner nor electronic prescription application provider has any way of knowing which intermediaries are used by each of the pharmacies that patients' may designate.

None of the security measures that are used for transmission address the threat of someone stealing a practitioner's identity to issue prescriptions or of office staff being able to issue prescriptions in a practitioner's name because of inadequate access controls or authentication protocols. None of the measures address the threat of pharmacy staff altering records to hide diversion. Some commenters indicated that they anticipate the elimination of intermediaries once the SCRIPT standard is mature and interoperability exists without the need for converting a data file from one software version to another so that it can be read correctly.

Although DEA is concerned about the possibility that controlled substances prescriptions could be altered or created during transmission, it has chosen to address those issues by requiring that the controlled substance prescription is digitally signed when the practitioner executes the two-factor authentication protocol and when the pharmacy receives the prescription. The only transmission issues that DEA is addressing in the interim final rule concern one common practice – the conversion of prescriptions from one software version to another – and one possible practice – the facsimile transmission of prescriptions by intermediaries to pharmacies. As discussed above, DEA will permit intermediaries to convert controlled substances prescriptions from one software version to another; DEA will not allow intermediaries to transform an electronic

prescription for a controlled substance into a facsimile as many of them do. DEA is also explicitly stating that any DEA-required information may not be altered during transmission.

H. Pharmacy Issues

1. Digital Signature

DEA proposed that either the pharmacy or the last intermediary routing an electronic prescription should digitally sign the prescription and the pharmacy would archive the digitally signed record as proof of the prescription as received.

Comments. State pharmacist associations and some pharmacy application providers asked DEA to analyze the cost of this requirement. One retail association stated that DEA had not considered that the software used to create the prescription might not be compatible with digital signatures. A number of pharmacy chains and pharmacy associations asked DEA to explain what regulatory requirements would apply to those electronic prescriptions that occur through direct exchanges between practitioners and pharmacies (i.e., transmission without intermediaries). A chain pharmacy noted that the intermediaries may be phased out, leaving pharmacies with no choice but to add digital signature functionality. A State Board of Pharmacy stated that the digital signature should be validated to ensure that the record had not been altered. An electronic prescription application provider stated that it will be very difficult for the pharmacies to digitally sign prescriptions in the short run and will require more time. It suggested that the rule include the following statement: "Until 1/1/2011 pharmacies can print out and wet sign controlled drug prescriptions as they arrive, and archive those paper records for an acceptable period." A standards organization stated that the requirement would

require a major revision of its standard. A healthcare system recommended that DEA include reasonable alternatives to proposed requirements to address record integrity. This commenter asserted that DEA should allow flexibility regarding the use of digital signatures in systems with no intermediate processing.

DEA Response. DEA did analyze the cost of this requirement in the Initial Economic Impact Analysis associated with the notice of proposed rulemaking[24] and included estimates for the time and costs required to add digital signature functionality to existing applications. DEA disagrees with the commenters that asserted that electronic prescribing applications or the SCRIPT standard are incompatible with digital signatures. As a number of commenters noted, any data file can be digitally signed and can be digitally signed without affecting the formatting of the file.

The interim final rule requires the pharmacy or the last intermediary to digitally sign the prescription and the pharmacy to archive the digitally signed record. These steps do not alter the data record that the pharmacy application will read. If the last intermediary digitally signs the record, the digital signature will be attached to the data record. Digital signatures, which under current NIST standards range from 160 to 512 bits (which generally equates to 20 to 64 bytes), would fit within the free-text fields that the SCRIPT standard provides (70 characters), or the digital signature could be linked to the prescription record rather than incorporated into the record. If the pharmacy digitally signs the prescription record, the issue of potential problems with the format will not apply. The digitally signed prescription-as-received record ensures that DEA can determine whether a prescription was altered during transmission or after receipt at the

[24] http://www.deadiversion.usdoj.gov/fed_regs/2008/index.gtml

pharmacy. If the contents of the digitally signed record at the pharmacy do not match the contents of the digitally signed record held by the practitioner's electronic prescription application, the prescription was altered during transmission. If the record of the prescription in the pharmacy database does not match the digitally signed record of the prescription as received, the prescription was altered after receipt.

About a third of registered pharmacies already have the ability to digitally sign electronic controlled substance orders through DEA's Controlled Substances Ordering System; the private key used for these electronic orders could be used to sign prescriptions upon receipt. Similarly, most applications that move files through virtual private networks or that conduct business over the Internet have digital signature capabilities. DEA has not imposed any requirements for the source of the digital signatures because pharmacies and intermediaries may already have signing modules that can be used. Pharmacies that have a Controlled Substance Ordering System digital certificate obtained it from DEA. In response to the comment on validating the digital signature, the pharmacy or intermediary will be signing the record; DEA sees no need to ask them to validate their own certificate. DEA does not believe that it is necessary to provide an alternative to the digital signature because it should be possible for either the intermediary or pharmacy to apply a digital signature within a reasonable time.

On the issue of direct exchanges between a practitioner and a pharmacy, two digital signatures (the electronic prescription application's or practitioner's and the pharmacy's) would be required unless the practitioner's digital signature is transmitted to the pharmacy and validated. Even when intermediaries are not involved, there is the possibility that an electronic prescription could be intercepted and altered during

transmission. When it becomes feasible for practitioners to transmit electronic prescriptions directly to pharmacies, without conversion from one software version to another, the PKI option that DEA is making available under the interim final rule may be an alternative that more applications and practitioners choose to use. The primary barrier to this option is the current need to convert prescription information from one software version to another during transmission because of interoperability issues; conversion of the prescription information from one software version to another makes it impossible to validate the digital signature on receipt. When interoperability issues have been resolved, transmitting a digital signature and validating the digital signature may be more cost-effective for some pharmacies. Because of the alternatives DEA is providing for practitioner issuance of electronic prescriptions for controlled substances, DEA does not believe it is necessary to develop alternative approaches that would apply only to those few truly closed systems. DEA notes that it has also made a number of changes to the proposed rule that are consistent with the practices described by the commenters from closed systems; for example, DEA is allowing institutional practitioners to conduct identity proofing in-house.

2. Checking the CSA database

DEA proposed that pharmacies would be required to check the CSA database to confirm that the DEA registration of the prescriber was valid at the time of signing.

Comments. Several commenters objected to this requirement, stating that pharmacies are not required to check DEA registrations for paper prescriptions unless they suspect something is wrong with a prescription. They also stated that the requirement would be costly and probably not feasible because the CSA database must be

purchased and is not up-to-date. Some commenters expressed the view that since DEA proposed to have electronic prescription application providers check the registration, requiring the pharmacy to do so would be redundant.

DEA Response. DEA agrees with those commenters that expressed the view that, when filling a paper prescription, it is not necessary for a pharmacist who receives an electronic prescription for a controlled substance to check the CSA database in every instance to confirm that the prescribing practitioner is properly registered with DEA. Accordingly, DEA has removed this requirement from the interim final rule. It should be made clear that a pharmacist continues to have a corresponding responsibility to fill only those prescriptions that conform in all respects with the requirements of the Controlled Substances Act and DEA regulations, including the requirement that the prescribing practitioner be properly registered. Pharmacists also have an obligation to ensure that controlled substance prescriptions contain all requisite elements, including (but not limited to) the valid DEA registration of the prescribing practitioner. If a pharmacy has doubts about a particular DEA registration, it can now check the registration through DEA's Registration Validation Tool on its Web site rather than having to purchase the CSA database.[25]

3. Audit Trails

DEA proposed that pharmacy applications have an internal electronic audit trail that recorded each time a controlled substance prescription was opened, annotated,

[25] DEA provides a "Registration Validation" tool on its Web site, through which DEA registrants may query DEA's registration database regarding another DEA registrant to gather specific information about that registrant. Information available includes: the registrant's name, address, and DEA registration number; the date of expiration of the registration; business activity; and the schedules of controlled substances the registrant is authorized to handle.

altered, or deleted and the identity of the person taking the action. The pharmacy or the application provider would establish and implement a list of auditable events that, at a minimum, would include attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with application operations in the pharmacy application. The application would have to analyze the audit logs at least once every 24 hours and generate an incident report that identifies each auditable event. Security incidents would need to be reported within one business day.

Comments. A substantial number of commenters representing pharmacies and pharmacy associations objected to the requirement that the audit trail document any time a prescription record was viewed, asserting that current applications do not have the capability to track this as opposed to tracking annotations, modifications, and deletions.

DEA Response. In view of the comments, DEA agrees that the audit function does not need to document every instance in which a prescription record is opened or viewed and has revised the rule accordingly. The pharmacy application will only be required to document those instances in which a controlled substance prescription is received, annotated, modified, or deleted. In such circumstances, the application must record when the annotation, modification, or deletion occurred and who took the action.

Comments. Several commenters stated that standards for the automation of capturing auditable events and interpretation of the resulting reports have not been published. Commenters asserted that many pharmacy applications have the ability to track auditable events, but not all have the ability to generate the reports desired by DEA. A number of commenters asked DEA to define auditable event and explain what level of security incident would need to be reported. A chain pharmacy asked DEA to define

what constituted an alteration of the record and to clarify that a generic substitution is not an auditable event. An application provider asked if auditable events are limited to information changed at the order level (e.g., administration instructions) or at dispensing (e.g., NDC changed due to insufficient quantity). A number of commenters suggested that reporting of security incidents should be within 2 to 3 business days.

DEA Response. The audit trail and the internal auditing of auditable events serve somewhat different purposes. The audit trail provides a record of all modifications to the prescription record. For example, the audit trail will note when the prescription was dispensed and by whom; it will indicate modifications (e.g., partial dispensing when the full amount is not available, changes to generic version). The auditable events, in contrast, are intended to identify potential security concerns, such as attempts to alter the record by someone not authorized to do so or significant increases in the dosage unit or quantity dispensed without an additional annotation (e.g., indicating practitioner authorization). DEA points out that during hearings on electronic prescriptions, representatives of the pharmacy and electronic prescription application industries uniformly stressed the audit trails as the basis for the security of their applications.

DEA does not believe it is feasible to define or list every conceivable event that would constitute an auditable event for all pharmacies. The extent to which a particular event might raise concern at one pharmacy is not necessarily the same at other pharmacies. For example, a community pharmacy may want to set different triggers for changes to opioid prescriptions than a pharmacy that serves a large cancer center or a pharmacy that services LTCFs would. A community pharmacy that is closed overnight may want to identify any change that occurs during the hours when it is closed – an event

that is not a consideration for a pharmacy that is open 24 hours a day. The auditable events must, at a minimum, include attempted or successful unauthorized access, modification, or destruction of information or interference with application operations in the pharmacy application. DEA has dropped the unauthorized "use or disclosure" from its list of auditable events. These events are included in the CCHIT standards for electronic health records and may be important to pharmacies, but are not directly relevant to DEA's concerns.

DEA expects that application providers and developers will work with pharmacies to identify other auditable events. DEA emphasizes that application providers should define auditable events to capture potential security threats or diversion. Changes from brand name drug to a generic version of the same drug, for example, do not represent potential security issues.

Comments. One State recommended that audit trails and event logs should be in a standard format.

DEA Response. DEA understands the State's desire for a uniform format for audit trails and event logs, but in the absence of a single industry-wide standard being utilized by pharmacies, DEA does not believe it would be appropriate at this time to mandate one particular format over others.

Comments. A pharmacy organization and pharmacist associations asked if audit trails and daily audits could be automated. One commenter asked DEA to clarify that the records could be kept on existing systems. Another asked if a pharmacy had to document that the record had been reviewed.

DEA Response. Audit trails and daily audits are automated functions that occur on the pharmacy's computers and that should not require actions on the part of pharmacists or other pharmacy employees except when a security threat is identified, which DEA expects to occur relatively rarely. The internal audit trail records must be maintained for two years, but DEA is not requiring that the pharmacy retain a record of its review of reports of auditable events unless they result in a report to DEA of a potential security incident.

Comments. A chain pharmacy asserted that as the record as received will be digitally signed, only a compromise of the encryption key should be an auditable event.

DEA Response. The digital signature on a record as received does not address the concerns that the audit trail and review are intended to document. The digitally signed prescription as received documents the information content of the prescription on receipt. It does not help identify later alterations of the record; it can show that the record was altered later, but not who did it or when.

Comments. A State asked if pharmacies should discontinue accepting electronic prescriptions if a security incident occurs.

DEA Response. In general, it would be advisable to discontinue accepting electronic prescriptions for controlled substances until the security concerns were resolved. However, if, despite the security concerns associated with the application, the pharmacy is able to verify that a prescription has been issued lawfully, the pharmacy may fill the prescription.

4. Offsite Storage

DEA proposed that back-up records be stored at a separate offsite location. DEA proposed that the electronic record be easily readable or easily rendered into a format that a person could read and must be readily retrievable.

Comments. Most pharmacy commenters objected to offsite storage as costly and not required for paper prescriptions. A pharmacy organization stated that back-up copies should be transferred off-site weekly, not daily.

DEA Response. DEA has removed the requirement for storage of back-up records at another location. DEA, however, recommends as a best practice that pharmacies store their back-up copies at another location to prevent the loss of the records in the event of natural disasters, fires, or system failures.

DEA believes that daily backup of prescription records is an acceptable length of time to ensure the integrity of pharmacy records.

Comments. Several pharmacy chains asked that the functionality for retrieving records be at the headquarters rather than the pharmacy level; they supported the standard of "readily retrievable," as DEA proposed, which is the same standard that applies to paper prescriptions. One State board of pharmacy stated that the provision for making the data available in a readable format may require extensive reprogramming. A pharmacist association asked DEA to define readily retrievable. One commenter objected to storing information at pharmacies because it could be exposed.

DEA Response. Under the interim final rule, it is permissible for a pharmacy to have records stored on headquarters' computers, but the dispensing pharmacy must be able to retrieve them if requested as they do for computerized refill records allowed under

§ 1306.22. DEA does not believe that the requirement for readable records will impose significant burdens. Similar requirements exist for computerized refill records. In addition, it is unlikely that pharmacy applications would be useable by pharmacists unless the data can be provided in an easily readable form. "Readily retrievable" is already defined in § 1300.01. Finally, requirements currently exist for pharmacies to retain and store prescription records in compliance with HIPAA requirements to protect individuals' personal information.

5. Transfers

In the NPRM, DEA confirmed existing regulations regarding the transfer of prescriptions for Schedule III, IV, and V controlled substances. Specifically, under § 1306.25(a) a pharmacy is allowed to transfer an original unfilled electronic prescription to another pharmacy if the first pharmacy is unable to or chooses not to fill the prescription. Further, a pharmacy is also allowed to transfer an electronic prescription for a Schedule III, IV, or V controlled substance with remaining refills to another pharmacy for filling provided the transfer is communicated between two licensed pharmacists. The pharmacy transferring the prescription would have to void the remaining refills in its records and note in its records to which pharmacy the prescription was transferred. The notations may occur electronically. The pharmacy receiving the transferred prescription would have to note from whom the prescription was received and the number of remaining refills.

Comments. Several commenters, including three pharmacy chains and an association representing chain drug stores, all indicated their belief that if a prescription transfer occurs within the same pharmacy chain, only one licensed pharmacist is

necessary to complete the transfer if that pharmacy chain uses a common database among its pharmacies. One pharmacy chain noted that in many cases, pharmacists do not call each other to effectuate the transfer of the prescription from one pharmacy to another. Commenters requested that DEA revise the rule to address this industry practice.

DEA Response. DEA has never permitted the transfer of a controlled substance prescription without the involvement of two licensed pharmacists, regardless of whether the two pharmacies share a common database. DEA emphasizes that this has been a longstanding requirement, one which was not proposed to be changed as part of this rulemaking. DEA believes that it is important that two licensed pharmacists be involved in the transfer of controlled substances prescriptions between pharmacies so that the pharmacists are aware that the prescription is actually being transferred. As the dispensing of the prescription is the responsibility of the pharmacist, DEA believes that it is critical that those pharmacists have knowledge of prescriptions entering their pharmacy for dispensing. Without this requirement, it would be quite feasible for other pharmacy employees to move prescriptions between pharmacies, thereby increasing the potential for diversion by pharmacy employees.

Comments. One commenter, a large pharmacy, believed that while the NPRM addressed the transfer of prescription refill information for Schedule III, IV, and V controlled substance prescriptions, it did not address the transfer of original prescriptions that have not been filled.

DEA Response. As DEA explained in the NPRM, the existing requirements for transfers of Schedule III, IV, and V controlled substances prescriptions remain unchanged. DEA currently permits the transfer of original prescription information for a

prescription in Schedules III, IV, and V on a one-time basis. This allowance does not change. DEA wishes to emphasize that the only changes made to § 1306.25 as part of the NPRM were to revise the text to include separate requirements for transfers of electronic prescriptions. These revisions were needed because an electronic prescription could be transferred without a telephone call between pharmacists. Consequently, the transferring pharmacist must provide, with the electronic transfer, the information that the recipient transcribes when accepting an oral transfer.

6. Other Pharmacy Issues

Comments. An advocacy group stated that although it expects the chain drug stores to be able to handle the administrative burden and expense of security measures demanded by DEA, it was concerned about the ability of independent pharmacies, especially those that rely almost exclusively on prescription revenues and not "front-of-the-store" revenues, to cope with the proposed rule's added requirements.

DEA Response. DEA has revised some of the requirements to reduce the burden imposed by this rulemaking, where DEA believes that doing so does not compromise effective controls against diversion. DEA has also clarified that the third-party audit applies to the application provider, not to the individual pharmacy unless the pharmacy has developed and implemented its own application, a circumstance which, at the present time, is likely limited to chain pharmacies. The audit trail is something that members of industry stated, prior to the proposed rule, was the basis for their security controls. The pharmacy applications should, therefore, have the capability to implement this requirement. DEA is simply requiring that the application identify security incidents, which should be infrequent, and that the pharmacy be notified and take action to

determine if the application's security was compromised. This should not be an insurmountable burden for a small pharmacy. The other functions required are automated and do not require action on the part of the pharmacy staff. Most of the burden of the pharmacy requirements fall on the pharmacy application provider, not on the pharmacy.

Comments. Some commenters stated that the requirements for paper prescriptions include, for practitioners prescribing under an institutional practitioner's registration, the specific internal code number assigned by the institutional practitioner under § 1301.22. These commenters stated that NCPDP SCRIPT does not accommodate the extensions, which do not have a standard format, nor do most pharmacy computer applications. They also noted that a pharmacy has no way to validate the extension numbers.

DEA Response. DEA is aware of the issue with extension data and published an Advance Notice of Proposed Rulemaking (74 FR 46396, September 9, 2009) to seek information that can be used to standardize these data and to require institutional practitioners to provide their lists to pharmacies on request. As discussed above, DEA believes that SCRIPT can be modified to accept extensions by adding a code that indicates that the DEA number is for an institutional practitioner and allowing the field to accept up to 35 characters. Pharmacy applications will need to be revised to accept the longer numbers; without the extension data, there is no way to determine who issued the prescription if individual practitioners with the same name are associated with the institutional practitioner. DEA is not requiring pharmacies to validate the extension

numbers unless the pharmacist has reason to suspect that the prescription or prescribing practitioner are not legitimate.

Comments. A pharmacy organization asked if a pharmacy that services a Federal healthcare facility would need to operate separate systems, one for Federal facilities and one for other facilities it serves. It also asked what facilities were considered Federal healthcare facilities.

DEA Response. As discussed above, DEA is allowing any application to use the digital certificate option proposed for Federal healthcare systems. DEA is not, therefore, imposing any different requirements on Federal facilities. Pharmacies may decide whether they will accept and verify digital signatures transmitted with a prescription, whether it was signed by a practitioner at a Federal facility or in private practice. If a pharmacy does not accept controlled substance prescriptions digitally signed with the individual practitioner's private key, it will have to ensure that it has a digitally signed record of the prescription as received. The rest of the requirements for annotating and dispensing a controlled substance prescription are the same for all electronic prescriptions for controlled substances. The determination of whether a particular facility is a Federal facility is not affected by this rulemaking.

I. Third Party Audits

DEA proposed that both electronic prescription applications and the prescription processing module in pharmacy applications should be subject to a third-party audit that met the requirements of SysTrust or WebTrust audits (or for pharmacies, SAS 70). The standards for these audits are established and maintained by the American Institute of

Certified Public Accountants.[26] [27] The audits are conducted by CPAs. DEA proposed that the application provider would have to have the third-party audit for processing integrity and physical security before the initial use of the application for electronic controlled substance prescriptions and annually thereafter to ensure that the application met the requirements of the rule. DEA sought comments on whether alternative audit types were available and appropriate.

Comments. An application provider organization stated annual security audits are unrealistic and will not be performed or enforced. The commenter asserted that a better use of both DEA and application provider resources would be to write and enforce a set of standards around systems writing.

DEA Response. Even if DEA had the technical expertise to develop standards, DEA does not believe that imposing an inflexible regulatory standard on applications is a reasonable approach. Security technologies are evolving. Locking applications into a specific format that would then have to be used until the regulation was revised, a time-consuming process, could delay implementation of more user-friendly and efficient applications that may be developed. In addition, most pharmacy applications have been in use for years; forcing them to reprogram in a specified way could be more costly and disruptive than letting each application provider tailor a solution that works for a particular application. DEA is interested in the end result (a secure system that can reasonably be implemented and is consistent with maintenance of effective controls against diversion of controlled substances), not in the details of how they are achieved.

[26] http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_06_3_party.html
[27] http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_06_3_party.html

DEA proposed third-party audits as a way to provide registrants with an objective appraisal of the applications they purchase and use. As a number of commenters stated, except for registrants associated with very large practices, large healthcare systems, or chain pharmacies, any of which may have their own information technology departments, the majority of registrants cannot be expected to determine, on their own, whether an application meets DEA's requirements. If they are to have assurance that the application they are using is in compliance with DEA regulatory requirements, that assurance must come from another source.

As commenters noted, DEA essentially had to choose among four possibilities for determining whether an application meets the requirements of part 1311: the application provider could self-certify the application; DEA could review and certify applications; an independent certification organization could take on that role; or the application provider could obtain a third-party audit from a qualified independent auditor. DEA believes that self-certification would not provide any assurance to registrants as non-compliant application providers would have an incentive to misrepresent their compliance with DEA regulatory requirements, and registrants would have few ways to determine the truth. For example, an application provider could claim that its application required the setting of logical access controls when the application, in fact, allowed anyone access regardless of the logical access controls. Until a practitioner or pharmacy discovered that prescriptions were being written or altered by unauthorized persons there would be no reason to suspect a problem with the application.

DEA does not have the expertise or the resources to conduct technical reviews of electronic prescription or pharmacy applications. Even if DEA elected to obtain such

expertise, the time required for it to do so and then to review all of the existing applications would delay adoption.

DEA believes that a third-party audit approach allows application providers to seek a review as soon as their applications are compliant, which should make applications available for electronic prescribing of controlled substances sooner than relying on DEA. Third-party audits, while perhaps new to some prescription and pharmacy application providers, are a common approach used by the private sector to ensure compliance with both government regulations and private sector standards. For example, the International Standards Organization (ISO) frequently requires companies to obtain a third-party audit to gain certification for compliance with its standards (e.g., ISO 9001, ISO 14001).[28]

The fourth approach would be to rely on an independent certification organization, such as CCHIT, to test and certify electronic prescription and pharmacy applications. Under the interim final rule, DEA will allow the certifications of such independent organizations to substitute for a third-party audit if the certification process clearly determines that the application being tested is compliant with DEA regulatory requirements and clearly distinguishes between applications that are compliant with part 1311 and those that are not. DEA notes, for example, that CCHIT currently tests and certifies EHRs against a set of published standards and plans to test and certify stand-alone electronic prescribing applications. However, at this time, CCHIT does not evaluate pharmacy applications. Once any certification organization has incorporated tests for part 1311 compliance, DEA will work with the organization to determine whether the process and certification are sufficient so that a registrant purchasing an

[28] http://www.iso.org/iso/iso_catalogue/management_standards/certification.htm

application can rely on the certification to ensure that the application is compliant. Because many application providers seek certification, this approach will reduce costs. DEA notes, however, that it has not been able to identify any independent organization that certifies pharmacy applications or any that certifies prescription modules at the level of detail DEA requires.

Comments. Two commenters asserted that third-party audits are not a common practice and not required for paper prescriptions.

DEA Response. Third-party audits, in this context, address the ability of the electronic prescription application or pharmacy application to handle controlled substance prescriptions securely. It is difficult to understand how that concept could be applied to paper prescriptions, where the only issues are whether they are written in compliance with the law and regulations, properly filed, and whether they have been altered. On a paper prescription, the alteration creates forensic evidence of the change, which is not necessarily the case with a prescription generated using an electronic application, where the lack of an audit trail or an audit function that has been disabled may eliminate any evidence of alterations.

Comments. Many of the commenters on this issue focused on the costs associated with third-party audits. One electronic prescription application provider that currently obtains a SysTrust audit stated that the cost of the audit for the proposed requirements would be considerably less than DEA had estimated. This commenter estimated the cost to be "in the lower tens of thousands of dollars range" rather than the range of $100,000 to $125,000 that DEA mentioned in the NPRM. Another electronic prescription

application provider asserted that the cost was underestimated and said the requirement would place a burden on application providers.

A pharmacy organization stated application vulnerabilities should be addressed through technology and that they should not create extra paperwork. It also stated that DEA should ensure that the cost of these audits is reasonable for small practices and pharmacies. A pharmacy organization and an information technology organization stated that the audit requirement is a burden financially and logistically. These commenters noted that some clinics that serve as both practitioners and pharmacies will bear the costs of both sides of the transaction.

DEA Response. DEA emphasizes that the requirement for a third-party audit applies to the application provider, not to the practitioner or pharmacy that uses the application. Unless a healthcare system or a pharmacy has developed its own application, it would not be subject to the requirement. Healthcare systems that serve as both practitioner and pharmacy may obtain a single third-party audit that addresses part 1311 compliance of the integrated system.

DEA has taken a number of steps to reduce the cost of the third-party audit. First, recognizing that the electronic prescribing and prescription processing functions DEA is requiring may not change every year, DEA has revised the rule to require an audit whenever an application is altered in a way that could affect the functionalities within the electronic prescription or pharmacy application related to controlled substance prescription requirements or every two years, whichever occurs first. Second, DEA has clarified that the purpose of the third-party audit is to determine whether the application meets DEA's requirements, that is, that the application is capable of performing the

functions DEA requires and does so consistently. Where the application is installed on practice or pharmacy computers, the audit will not need to address the application provider's physical security nor will it need to address physical security at the practice or pharmacy because that will vary with each installation and is beyond the control of the application provider. For application service providers, the physical security of the ASP will need to be audited.

Third, as discussed above, if independent certification organizations develop programs that certify applications for part 1311 compliance, DEA will review their processes to determine whether such certifications can substitute for a third-party audit.

Finally, DEA has expanded the kinds of third-party auditors beyond those who perform SysTrust, WebTrust, or SAS 70 audits to include certified information system auditors (CISA) who perform compliance audits as a regular ongoing business activity. The CISA certification is sponsored by the Information Systems Audit and Control Association (ISACA)[29] and is recognized by the American National Standards Institute under ISO/IEC 17024. The certification is required by the FBCA for third-party auditors and by the Federal Reserve Bank for its examiners and is approved by the Department of Defense. DEA believes that allowing other certified IT auditors will provide application providers with more options and potentially reduce the cost of the audit. DEA is seeking comments on the addition of CISA to the list of permissible auditors.

Comments. A mail-order pharmacy said the rule should state that the annual SysTrust or SAS 70 audit meets DEA's regulatory requirements so that pharmacies

[29] http://www.isaca.org

passing their most recent audit can begin accepting electronic controlled substance prescriptions.

DEA Response. The SysTrust or SAS 70 audit will be sufficient if the audit has determined that the application meets the applicable requirements of part 1311. Because the pharmacy requirements address internal audit trails, logical access controls, and the ability to annotate and retain prescription records, which may be standard functions in existing pharmacy applications, it is possible that the existing audit has covered these functions. The pharmacy and the auditor should review the requirements of part 1311 and determine whether compliance has been addressed by the existing audit.

Comments. An intermediary suggested that certifying organizations such as itself and CCHIT could make the presentation of the audit a condition of certification. An information technology organization suggested that DEA might consider the North American Security Products Organization (NASPO) certification as a recognized standard for security products since, the commenter asserted, NASPO certification is sponsored by the FBI and Secret Service through the Document Security Alliance.

DEA Response. DEA notes that the commenter's existing certification process does not address the functions that DEA is requiring, but rather focuses on compliance with the SCRIPT standard. The commenter, as it stated, would rely on third-party audits to determine whether the applications meet DEA's requirements. Although the commenter may choose to impose this requirement on entities it certifies, making the third-party audit a condition of certification by this intermediary would not reduce the cost for the application providers because they would still need to obtain a third-party audit. Further, DEA cannot rely on one third party's certification of another third party's

audit or certification of a particular application's compliance with DEA regulatory requirements. In this regard, DEA must look to its own regulatory authority and regulatory requirements, not those of other entities. This is particularly true as DEA is not mandating the use of intermediaries.

As discussed above, if a certification organization decides to incorporate, as part of its certification, a determination that the application meets the requirements of part 1311, DEA will review the process used to determine whether the certification can be used as a substitute for a third-party audit. Based on a review of the information available on its Web site,[30] NASPO does not appear to address applications such as those used to create electronic prescriptions, but rather certifies organizations. Thus, DEA does not believe that NASPO is currently a suitable alternative to the third-party audits or certifications DEA is requiring in this rule.

Comments. Some commenters stated that there are multiple versions of applications in use and that third-party audits would not be feasible in these cases.

DEA Response. The existing certification programs test and certify multiple versions of applications. The application providers should, therefore, be familiar with the process of gaining approval for new versions. DEA notes that it is requiring a new audit more frequently than once every two years only when one of the functions required by part 1311 is affected by an update or upgrade to the application. If an application provider has multiple versions of the application, all of which use the same code and controls for the functions that DEA is requiring, a single audit may be able to address multiple versions if other changes could not impact these functions.

[30] http://www.naspo.info

Comments. Some commenters thought that individual practitioners or pharmacies would have to obtain an audit of their applications.

DEA Response. As discussed above, a practice or pharmacy will be required to obtain an audit only if it developed the application itself. Although there may be some pharmacy chains that developed their own applications, it appears that even large hospital systems usually obtain applications from application providers. If the application provider has tailored its application to meet the specific needs of a healthcare system or a pharmacy chain, the application provider will have to determine whether the changes it made for a particular client affect the capability of the application to meet DEA's requirements. If the healthcare system or pharmacy-specific changes do not affect the functions specified in part 1311, a single audit may be able to address the multiple tailored versions of its application. DEA expects that, except for very large healthcare systems or practices, applications will not be tailored in ways that will affect compliance with part 1311.

Comments. One application provider stated that some of the controls that DEA wants addressed in the audit are not under the application provider's control when the application has been installed on a practice or pharmacy computer.

DEA Response. DEA recognizes that the proposed rule failed to address adequately the different roles played by application providers that install applications and those that serve as application service providers. To address the differences, DEA has revised the rule to clarify that a third-party audit does not need to address physical security of an application provider if its application is installed on practitioner office or pharmacy computers and servers. The audit for applications that will be installed on

practice or pharmacy computers is limited to the application's ability to meet the part 1311 application requirements. The application provider, in this case, has no control over physical security of the application installed at the practice or pharmacy location and the security of its own operations is not of concern to DEA because the prescription records are not created or stored on computers that the application provider controls. A third-party audit for an application service provider, whose servers and Web sites host the files of practices or pharmacies, must, however, address physical security because the ability of the ASP to prevent insider and outsider attacks is critical to the security of prescription processing.

Comments. Pharmacy commenters stated that SureScripts/RxHub certification and HIPAA compliance should be sufficient to meet DEA regulatory requirements. One pharmacy chain asserted that it should be allowed to self-certify that its pharmacy application was compliant with DEA requirements for electronic prescriptions. Two retail pharmacy associations stated that the rule was not needed for pharmacies because State pharmacy boards may inspect their computer applications. They stated that their applications must comply with HIPAA and the SCRIPT standard. A State agency stated that these audits for pharmacies may not be needed and would impose additional costs on pharmacies.

DEA Response. SureScripts/RxHub certifies pharmacy and electronic prescription applications for interoperability and compliance with NCPDP SCRIPT, but not for their internal security or other functionalities; as commenters noted, SCRIPT supports, but does not mandate, the inclusion of all the DEA-required information. In addition, SureScripts/RxHub is not a neutral third party, but was established and is run by

the pharmacy industry and may have a vested interest in promoting the existing model of transmission over others. Thus, DEA believes that SureScripts/RxHub certification, while beneficial from an industry perspective, is not suitable to address DEA's requirement for a neutral unbiased third-party audit of electronic prescription and pharmacy applications. DEA also notes that assertions (especially self-assertions, which are typically not verified by an outside party) of compliance with the HIPAA Security Rule provide limited assurance of security. The HIPAA Security Rule, which is focused on protecting personal health information from disclosure, is risk-based and designed to be flexible and scalable because the risks may vary with the number of patients. In contrast, DEA has based its requirements on its statutory obligations and must require all pharmacies to implement the defined security controls. As discussed above, application provider self-certification would not provide registrants with reasonable assurance of compliance.

DEA would be willing to evaluate a request from a pharmacy board to carry out a third-party audit or review of an audit, but as no State Board offered to take on this role in its comments to the NPRM, DEA doubts that this approach is feasible.

Comments. An application provider stated that the SysTrust and WebTrust audits are intended for e-commerce Web sites. The commenter asserted that a healthcare information application is considerably more complex than an e-commerce Web site, as an EMR may provide thousands of features/functions. The commenter asked what the auditor would examine and test during an audit of such a complex application. The commenter asked whether CPA firms are qualified to audit such complex applications in a consistent manner. With the overall complexity and the number of organizations that

would be required to obtain the audits, it asked whether DEA had considered the impact of such a requirement if organizations are not able to get an audit performed due to overall demand.

DEA Response. The WebTrust audit is intended for Web sites, but the SysTrust audit and the SAS 70 audits are not. DEA stated in the NPRM that the only aspects of the applications that are subject to the audit are processing integrity and, for ASPs, physical security as they relate to the creation and processing of controlled substance prescriptions. DEA is not requiring an application provider to have all aspects and functions of their applications audited. Although a provider may want an auditor to determine whether its application accurately moves data from one part of an EHR to another (e.g., diagnosis codes from the patient record to an insurance form), DEA is not requiring that such functions be audited unless they directly affect the creation, signing, transmitting, or, for pharmacies, the processing of controlled substance prescriptions.

As discussed above, if an organization develops a program to certify electronic prescription or pharmacy applications, DEA will review the processes for certification of applications proposed by that organization to determine if the certification standards adequately evaluate compliance with part 1311. DEA will provide a list of those organizations whose certification processes adequately address compliance with DEA's requirements and allow such certifications to take the place of third-party audits. This should reduce the cost to application providers. As for the concern about the availability of third-party auditors, DEA notes that there are a limited number of applications, which are unlikely all to be ready for audits at the same time. DEA, however, has expanded the range of potential auditors by including those who have CISA credentials.

Comments. A number of commenters objected to the annual audit, stating that the applications do not change annually. They suggested a two- or three-year period would be more appropriate.

DEA Response. DEA agrees with commenters on the issue of annual audits and has revised the rule to require an initial audit prior to use of the application for electronic prescriptions for controlled substances, and to require subsequent audits once every two years or whenever functions related to creating and signing or processing of controlled substance prescriptions are altered, whichever occurs first. Application providers will be required to keep their most recent audit report and any other reports obtained in the previous two years. DEA notes that CCHIT now requires recertification every two year.

Comments. Practitioner organizations, healthcare organizations, and an intermediary stated that prescribers are not competent to review audits and that DEA should publish a list of qualifying applications. One association stated that the onus should be on the application provider to meet the requirements and fix any deficiencies so that practitioners do not need to stop using an application.

DEA Response. SysTrust and WebTrust audit reports are intended for the public. It should not be difficult for an application provider to insist that the report include a summary that clearly states whether the application meets DEA requirements. If certification bodies take on the role of certifying applications for compliance with part 1311, the existence of the certification will be enough to meet the requirement to use a compliant application. DEA expects that application providers will have an incentive to address any shortcomings quickly to ensure customer satisfaction.

Comments. Another commenter asked why the intermediaries are not required to be audited. A State agency asserted that intermediaries should be independently certified and audited annually. That commenter suggested that transmission should be limited to wired networks.

DEA Response. DEA's rule does not address the use of intermediaries in the transmission of electronic prescriptions for controlled substances. Rather, it addresses requirements for applications used to write electronic prescriptions for controlled substances and process them at pharmacies, and requirements for the registrants who use those applications. DEA requires registrants to use only applications that meet certain requirements because the registrants choose the applications. Registrants have no control over the string of three to five intermediaries involved in some electronic prescription transmissions. A practitioner might be able to determine from his application provider which intermediaries it uses to move the prescription from the practitioner to SureScripts/RxHub or a similar conversion service, but neither the practitioner nor the application provider would find it easy to determine which intermediaries serve each of the pharmacies a practitioner's patients may choose. Pharmacies have the problem in reverse; they may know which intermediaries send them prescriptions, but have no way to determine the intermediaries used to route prescriptions from perhaps hundreds of practitioners using different applications to SureScripts/RxHub or a similar service. Despite these considerations, DEA believes the involvement of intermediaries will not compromise the integrity of electronic prescribing of controlled substances, provided the requirements of the interim final rule are satisfied. Among these requirements is that the prescription record be digitally signed before and after transmission to avoid the need to

address the security of intermediaries. DEA realizes that this approach will not prevent problems during the transmission, but it will at least identify that the problem occurred during transmission and protect practitioners and pharmacies from being held responsible for problems that may arise during transmission that are not attributable to them.

J. Risk Assessment

In the NPRM, DEA provided a detailed risk assessment, applying the criteria of OMB M-04-04, a guidance document for assessing risks for Federal agencies. (See 73 FR 36731-36739; June 27, 2008.) Under M-04-04, risks are assessed for four assurance levels (1 – little or no confidence in asserted identity – to 4 – very high certainty in the asserted identity) across six potential impacts. M-04-04 classifies risks as low, medium, and high as described in Table 1 and associates risk levels with assurance levels as shown in Table 2.

Table 1: M-04-04 Potential Impacts of Authentication Errors[31]

	Low Impact	**Moderate Impact**	**High Impact**
Potential Impact of Inconvenience, Distress or Damage to Standing or Reputation	At worst, limited short-term inconvenience, distress or embarrassment to any party.	At worst, serious short-term or limited long-term inconvenience or damage to the standing or reputation of any party.	Severe or serious long-term inconvenience, distress or damage to the standing or reputation to the party (ordinarily reserved for situations with particularly severe effects or which may affect many individuals).
Potential Impact of Financial Loss	At worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	At worst, a serious unrecoverable financial loss to any party, or a serious agency liability.	Severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.
Potential impact of harm to	At worst, a limited adverse effect on	At worst, a serious adverse effect on	A severe or catastrophic adverse effect on

[31] Office of Management and Budget. "E-Authentication Guidance for Federal Agencies" M-04-04. December 16, 2003.

	Low Impact	Moderate Impact	High Impact
agency programs or public interests	organizational operations, assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness; or (ii) minor damage to organizational assets or public interests.	organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of [sic] to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
Potential Impact of unauthorized release of sensitive information	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact, as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a moderate impact, as defined in FIPS PUB 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a high impact, as defined in FIPS PUB 199.
Potential Impact to Personal Safety	At worst, minor injury not requiring medical treatment	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
Potential impact of civil or criminal violations	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

Table 2: Maximum Potential Impacts for Each Assurance Level

	Level 1	Level 2	Level 3	Level 4
Potential Impact of Inconvenience, Distress, or Damage to Standing or Reputation	Low Impact	Moderate Impact	Moderate Impact	High Impact
Potential Impact of Financial Loss	Low Impact	Moderate Impact	Moderate Impact	High Impact
Potential impact of harm to agency programs or public	n/a	Low Impact	Moderate Impact	High Impact

	Level 1	Level 2	Level 3	Level 4
interests				
Potential Impact of unauthorized release of sensitive information	n/a	Low Impact	Moderate Impact	High Impact
Potential Impact to Personal Safety	n/a	n/a	Low Impact	Moderate Impact
Potential impact of civil or criminal violations	n/a	Low Impact	Moderate Impact	High Impact

In the risk assessment conducted as part of the NPRM, DEA determined that the potential impact of financial loss and the potential impact of unauthorized release of sensitive information were not applicable to the rule; the risk related to the potential impact of inconvenience, damage, or distress to standing or reputation was rated as moderate. DEA rated the other three factors as high risk, which is associated with Level 4. As DEA discussed in the NPRM, inadequate requirements for authentication protocols would make it difficult to detect diversion and to enforce the statutory mandates of the Controlled Substances Act; DEA's ability to carry out its statutory mandate would be seriously undermined. As DEA discussed extensively in the NPRM, the consequences of diversion and abuse of controlled substances are clearly severe to the users. The criminal penalties associated with diversion involve imprisonment and/or fines. (See 73 FR 36733-36734, June 27, 2009, for a full description of the reasons for DEA's ratings.) Because the highest risk level rated for any element determines the overall assurance level, DEA proposed using Level 4 for the authentication protocols although it did not apply any assurance level to identity proofing.

Comments. Only four commenters directly addressed the risk assessment. An application provider and an information technology firm addressed the requirements for a

hard token and asserted that Level 4 would be very hard to implement and that Level 3 would be sufficient.

The information technology firm stated that Level 4 token technology is significantly more costly to distribute, manage, and operate than multi-token Level 3 technologies. The commenter asserted that cell phone-based multi-factor one-time-password devices require the distribution of code that is unique to each cell phone platform. Consequently, the commenter asserted, the cost and complexity for the end-users is significant. The logistical management of the software and cryptographic solutions for multi-factor cryptographic hardware devices make their cost untenable in a large scale, heterogeneous deployment. The application provider asserted that Level 4 requires that every system user use a Level 4 token to access the system, not just practitioners accessing select functions in a single application. Both commenters suggested that DEA require Level 3 tokens that are stored on a device "separate from the computer gaining access," citing OMB memorandum M-07-16 on safeguarding personal information.[32] These commenters asserted that this approach would eliminate the risk that DEA cited with NIST Level 3, which allows storage on the computer gaining access. They stated that "the use of such multi-token level 3 two-factor authentication solutions has been proven successful in mass scale deployments with heterogeneous user populations since no hardware or software is required by the end-user specific to the authentication transaction. This has been done with no provisioning complexity and a variety of integrated identity proofing capabilities including face-to-face and remote knowledge-based identity proofing." An intermediary stated that most PDAs or other

[32] http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2007/m07-16.pdf

handheld devices typically do not meet a FIPS 140-2 validation with physical security at Level 3 or higher. It also said that SP 800-63-1 does not require that approved cryptographic algorithms must be implemented in a cryptographic module validated under FIPS 140-2.

DEA Response. DEA agrees with some of the comments and has revised the interim final rule to allow authentication protocols that meet NIST Level 3; if the protocols involve a hard token, they must be either one-time-password devices or cryptographic modules that are not stored on the computer the practitioner is using to access the application. Contrary to the commenter's claim, NIST SP 800-63-1 requires both OTP devices and cryptographic tokens to be validated at FIPS 140-2 Security Level 1 or higher.[33]

The primary purpose of the higher level of physical security for Level 4 is to prevent tampering with the device. Given the technical expertise needed to tamper with a device without making it nonfunctional, DEA does not consider that such tampering is enough of a risk in healthcare settings to justify imposing the higher costs associated with such devices. DEA believes that the other steps it is implementing regarding identity proofing and logical access control are sufficient to mitigate the risk to allow for Level 3 rather than Level 4 tokens. By requiring that two factors are used to access the controlled substance functions in the application, DEA is limiting the threat from stolen or tampered-with tokens.

Comments. Another application provider objected to DEA's assessment and argued that Level 2 protections (single-factor) were adequate. The application provider

[33] National Institute of Standards and Technology. Special Publication 800-63-1, Draft Electronic Authentication Guideline, December 8, 2008, pages 40-41.

stated that Level 2, with the use of a strong password in addition to a known Internet Protocol address or out-of-band token, would be sufficient. The application provider also suggested that DEA should adopt a tiered approach, with lesser requirements for Schedule III, IV, and V substances (just a strong password). For Schedule II, it suggested a combination of a strong password and other "something you know" (e.g., out-of-band message, challenge response questions) plus a printout of every prescription, with the printout manually signed to create an audit trail. As an alternative the application provider suggested that if DEA requires two-factor authentication, DEA should allow a variety of second factors including whitelisted IP address, biometrics, soft tokens, and hard tokens, such as proximity badges, barcode readers, thumb drives, etc.

DEA Response. DEA disagrees with this commenter. DEA does not believe that one-factor authentication is adequate. As discussed at length above, passwords are not secure, particularly in healthcare settings where people work in close proximity to each other and many people may use the same computers. Even without the possibility of shoulder-surfing in such settings, strong passwords, because of their complexity and the need to change them frequently, are more likely to be written down. DEA also notes that maintenance of password systems imposes considerable costs.

DEA also disagrees with the commenter's suggestion for different requirements for Schedule II prescriptions. As DEA has discussed, electronic prescriptions are written prescriptions. Requirements for written prescriptions are uniform, regardless of the schedule of the controlled substance. Further, to establish differing requirements for Schedule II controlled substance prescriptions as compared with Schedule III, IV, and V prescriptions would add unnecessary complexity to the electronic prescription

application. The commenter's suggestion appears to be based on the assumption that Schedule II substances, and their related prescriptions, are more likely to be diverted; however, DEA notes that both Schedule III and Schedule IV substances, and their related prescriptions, are regularly diverted for nonlegitimate use. DEA believes that a single approach more accurately reflects the statutory and regulatory requirements for written prescriptions, is more appropriate, and will be easier for application providers and practitioners to implement.

DEA has adopted some of the second factors that the commenter suggested, specifically the biometric and any hard token that meets NIST Level 3, which could include proximity cards and thumb drives that contain a cryptographic module. DEA does not believe that associating a prescription with a particular IP address will provide a pharmacy any assurance of the identity of the person who signed the prescription; any prescription generated on a practice's computers may have the same IP address. This suggestion also assumes that every pharmacy to which a practitioner may transmit would have the ability to determine whether the source IP address was whitelisted.

Comments. An intermediary asserted that DEA should implement electronic prescriptions for controlled substances with Level 2 and increase the requirements only if needed. The commenter asserted that the existing system includes authentication of the clinician and the connections, access controls, audit trails, and pharmacist as a gatekeeper. It stated that electronic prescribing could not increase the speed of diversion because the pharmacist acts as a gatekeeper. The commenter claimed that electronic prescribing would have a low impact on harm to the agency and public interest. The commenter asserted that the ability to breach the electronic prescribing infrastructure

would take far greater expertise than today's paper system. The commenter further claimed that electronic prescribing would reduce the risk of injury and death by reducing undetectable diversion and abuse. The commenter asserted that personal safety should be considered low risk. Stronger authentication of the clinician minimally reduces the risk of alteration of the prescription; existing processes and controls audited by third parties reduce the overall risk more significantly. The commenter believed that existing electronic prescribing infrastructure and systems will dramatically reduce the chance of diversion and abuse seen in the existing paper process; thus, the commenter asserted, the risk of civil or criminal violations is actually reduced with electronic prescribing and should be considered low. The commenter stated that data mining would effectively address diversion concerns.

DEA Response. DEA strongly disagrees with this commenter's claims. The existing system, where some applications allow individuals to enroll online with no identity proofing, provides no assurance that the person issuing a prescription is a practitioner. It takes no technical expertise to steal an identity, particularly for office staff who have access to DEA registration certificates and State authorizations. Applications that do not have logical access controls or do not implement them may allow any person with access to a practitioner's computers to write and issue prescriptions. Passwords, as discussed previously, are the most common form of authentication credential and provide no proof that the person entering the password is the person associated with the password. The security of the prescription as it moves through intermediaries is of limited value if there is no evidence of who issued the prescription. Strong authentication is needed, not simply to prevent alteration, but to prevent nonregistrants from issuing

controlled substance prescriptions. The risk of diversion without strong authentication is high. The practitioners could be subject to civil and criminal prosecution if their applications are misused and prescriptions are written in their names, or if their identity is stolen.

As to the claim that pharmacists will prevent wide-spread diversion, it is difficult to see how this could be the case. If someone issues multiple prescriptions to a patient and transmits them to multiple pharmacies, the pharmacists will have no ability to identify the problem, just as a single pharmacist will not be able to identify fraudulent prescriptions issued to multiple patients. Unlike paper prescriptions, electronic prescriptions lack many of the indications of a forged prescription that pharmacists use to identify a forged paper prescription. Electronic prescribing applications make it difficult for the person diverting to misspell a drug name or to select dosage forms that do not exist; they provide no indication of alterations.

The commenter assumes that such problems will be discovered through data mining and that data mining will reduce diversion. DEA, however, has no authority to collect data on all prescriptions issued and, therefore, no ability to conduct data mining. Even if DEA had the authority to collect prescription data, data mining would only work if all prescription data were available (electronic prescriptions, paper, fax, and oral) and in a common electronic format. If the per-prescription transaction fee charged by the commenter for transmission is any indication of the cost of that one step in data mining, the cost of data mining for controlled substance prescriptions to DEA could be high.

Data mining, were it legally possible and economically feasible, is based on being able to identify patterns of unusual activities. Data mining might detect individuals

diverting controlled substances for themselves or registrants issuing large numbers of prescriptions potentially other than for legitimate medical purposes. It would not identify the organized diverters who would easily determine what patterns would trigger investigation and avoid those patterns. One problem with poorly controlled or uncontrolled electronic prescription issuance is that it would be easy for criminals to steal practitioner identities, issue a limited number of prescriptions under each identity to a limited number of patients, and move on to the next set of stolen identities. Nothing in the pattern would trigger investigation, regardless of whether data mining was being conducted.

Finally, data mining, even in real time if that were to be possible, would not prevent many of the injuries and deaths diversion causes because the drugs would have been obtained and used or sold before law enforcement could act. To claim that the risk to personal safety is low is to ignore the reality of the consequences of drug diversion. DEA considers it critical that electronic prescribing applications for controlled substance prescriptions be designed to limit the possibility of diversion to as great an extent as possible rather than assume that the problems will not occur. Fixing the problem after electronic prescribing applications are widely deployed, as the commenter suggested could be done, would be far more difficult and more disruptive than implementing reasonable controls in the early stages of the applications' use.

Because of DEA's statutory responsibilities and the magnitude of the harm to the public health and safety that would result if an insufficiently secure system were to cause an increase in diversion of controlled substances, any regulations authorizing the use of electronic prescriptions for controlled substances must contain adequate security

measures from the outset. DEA cannot, consistent with its obligations, set the bar lower than it believes necessary with an eye toward increasing the security requirements at some later date should the vulnerabilities be exploited. Regulatory changes take significant time – time during which there could be continuing harm to the public health and safety.

Comment. One application provider stated that the use of the government guidelines for risk assessment was inappropriate because those guidelines were developed to analyze people remotely accessing open networks.

DEA Response. DEA recognizes that the guidelines were developed for government systems, but believes that the basic principles can be applied to the security of both Federal and private applications. Although practitioners may write most of their prescriptions while at their offices, they will probably want the ability to access their office applications when they are away from the office so they can issue prescriptions remotely when needed; such access will frequently be through the Internet and may use wireless connections. In addition, practitioners using application service providers access the electronic prescription application over the Internet, which they may do from any computer or location. Security concerns must address both of these situations.

K. Other Issues

1. Definitions

In the NPRM, DEA proposed to move all of the existing definitions in part 1311 to a new section in part 1300 (§ 1300.03) and to add new definitions to that section. The proposed definitions included "audit," "audit trail," "authentication," "authentication protocol," "electronic prescription," "hard token," "identity proofing," "intermediary,"

NIST SP 800-63," "paper prescription," "PDA," "SAS 70 audit," "service provider," "SysTrust," "token," "valid prescription," and "WebTrust."

Definition of "Service provider." In the NPRM, DEA proposed to define a service provider as follows:

> Service provider means a trusted entity that does one or more of the following:
> (1) Issues or registers practitioner tokens and issues electronic credentials to practitioners.
> (2) Provides the technology system (software or service) used to create and send electronic prescriptions.
> (3) Provides the technology system (software or service) used to receive and process electronic prescriptions at a pharmacy.

Comments. Practitioner and pharmacy organizations requested that DEA define service providers and intermediaries. A practitioner organization stated that DEA had used "service provider" for any third party (vendor or intermediary). It believed that these should have separate names. A standards organization asked who the service provider is in the case where the software is loaded to the practitioners' computers. A pharmacy organization also asked for clarification of the term "service provider" and whether their functions can be delegated.

An intermediary recommended modifying the definition of service provider to recognize that some prescribers and the entities for which they work have created their own electronic prescribing applications. The intermediary noted that some prescribers, as well as some pharmacies, have their own proprietary applications and do not connect to intermediaries through third-party service providers, but rather connect directly. Accordingly, some entities in fact act as both a prescriber or pharmacy, on the one hand, and an application provider, on the other hand. The intermediary also noted that the addition of the word "trusted" to the definition of service provider adds a subjective

element that is not defined anywhere in the NPRM. While the word "trusted" is a term of art used in the industry, since it is not defined in the NPRM, the intermediary stated that DEA should delete the word "trusted" from the definition of service provider to avoid any ambiguity in the future. The intermediary argued that if an entity complies with the requirements as imposed by the rule, then that entity is and should be considered a trusted entity, and there is no need to introduce an undefined and subjective word such as "trusted" into the definition.

DEA Response. DEA agrees that further delineation among the various entities involved in electronic prescribing of controlled substances is needed. In addition, DEA has changed the terms to use the more accurate word "application," rather than service or system. In computer terminology, an application is software that performs specific tasks (e.g., word processing, EHRs); a system is the underlying operating program. DEA has, therefore, revised the rule to add the following definitions.

Electronic prescription application provider means an entity that develops or markets electronic prescription software either as a stand-alone application or as a module in an electronic health record application.

Pharmacy application provider means an entity that develops or markets software that manages the receipt and processing of electronic prescriptions.

Application service provider means an entity that sells electronic prescription or pharmacy applications as a hosted service, where the entity controls access to the application and maintains the software and records on its servers.

Installed electronic prescription application means software that is used to create electronic prescriptions and that is installed on a practitioner's computers and servers, where access and records are controlled by the practitioner.

Installed pharmacy application means software that is used to process prescription information and that is installed on the pharmacy's computers or servers and is controlled by the pharmacy.

The definition of "intermediary" is unchanged from the NPRM: "Intermediary means any technology system that receives and transmits an electronic prescription between the practitioner and pharmacy."

DEA believes that these revisions will clarify the rule and allow DEA to make the distinction between application service providers, who host and manage the electronic prescription applications on an ongoing basis, and those providers that develop, market, or install software, but do not manage the application once it is installed. In the case of a closed system, a single entity may manage both the electronic prescription application and the pharmacy application and, therefore, would be considered to be the provider of both. Based on the inclusion of these new definitions, DEA has removed the term "service provider" from the interim final rule.

Definition of "electronic signature." In the NPRM, DEA proposed to define the term electronic signature as follows: "Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message." As DEA explained in the NPRM, this definition of electronic signature is taken directly from 21

CFR 1311.02, and was merely being merged into the definitions section for electronic ordering and prescribing activities.

Comments. Several commenters stated that DEA should adopt the E-Sign definition of electronic signature: "Electronic Signature means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."

DEA Response. DEA disagrees. The definition of "electronic signature" in the proposed rule is the existing definition in § 1311.02 that was adopted in 2005 when DEA promulgated its "Electronic Orders for Controlled Substances" Final Rule (70 FR 16901, April 1, 2005). DEA is simply moving the definitions codified in that final rule to a new section. DEA believes that the E-Sign definition is too general to provide the necessary clarity in the context of this interim final rule.

Comments. A healthcare group asked DEA to further define "manually signed." It asked whether the act of a practitioner signing with an electronic signature would suffice or is a handwritten signature on the computer-generated prescription that is printed or faxed required.

DEA Response. DEA does not believe that "manually signed" requires further definition. The phrase "manually signed" has been a part of the DEA regulations since the inception of the CSA (and is currently found in § 1306.05(a)) without the need for elaboration. It has a plain language meaning that is clear: the practitioner must use a pen, indelible pencil, or other writing instrument to sign by hand the paper prescription.

Comments. An application provider organization stated that the word "signing" is imprecise; instead it should say "approve" and/or "transmit."

DEA Response. DEA has revised the proposed rule, as discussed, to require that two-factor authentication act as signing and that the application must label the function as signing as well as presenting a statement on the screen that informs the practitioner that executing the two-factor authentication protocol is signing the prescription. Signing is the practitioner's final authorization for the transmission and dispensing of a controlled substance prescription, issued for a legitimate medical purpose in the usual course of professional practice, and indicating the practitioner's intent to be legally responsible for such authorization.

Comments. A State Board of Pharmacy provided definitions it uses for electronic prescriptions to define "point of care vendors," "network vendors," "prescribers," and "contracted."

DEA Response. DEA considered these definitions in developing its definitions for the interim final rule. The definitions offered by the Board of Pharmacy commenter include requirements, which are not generally part of Federal definitions. The commenter's definitions appear to rely on contracts among the various vendors for security, but it is not clear how these contracts would be enforced or how a practitioner or pharmacy would be able to determine that they were in place. DEA also notes that the network vendor definition fails to consider that many intermediaries connect only to other intermediaries, not to practitioners and pharmacies. A definition of prescriber is not needed as DEA's rules limit who can prescribe controlled substances. Thus, while DEA appreciates the Board of Pharmacy's suggestions, it did not adopt any of the definitions specifically included in the comment.

Definition of “closed system.” DEA did not propose to define the term "closed system." This phrase would refer to situations in which both the electronic prescription application and the pharmacy application were controlled by the same entity and where practitioners and pharmacies outside of the closed system could not access or be accessed by users of the closed system.

Comments. An insurance industry organization suggested that DEA add a definition of “closed system” to address healthcare systems that employ both the practitioner and pharmacists and handle the prescriptions within a single system.

DEA Response. DEA does not believe that a definition of closed system is needed at this time because DEA is not imposing any additional or different requirements on closed systems. Closed systems are subject to the same rules as open systems. As discussed above, DEA is allowing non-Federal systems to use the rules proposed for Federal systems. Some closed systems may find it advantageous to adopt this approach, but they are not required to do so.

Definition of “hard token.” In the NPRM, DEA proposed to define the term hard token as follows: “Hard token means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card) rather than on a general purpose computer."

Comments. An information technology organization recommended that DEA add a USB fob to the list of hardware devices described in the definition of hard token. It also recommended the use of the term Key Storage Mechanism instead of hard token as this is the more standard industry term in current use.

DEA Response. DEA has added USB fob to the list of devices described in the definition of “hard token.” DEA notes that this list merely provides examples and is not

all-encompassing. If another hardware device meets DEA's requirements for security it can be used to meet the requirements of this interim final rule.

Definitions related to digital signatures. DEA did not propose any definitions in the NPRM related to digital signatures other than those it was transferring from 21 CFR 1311.02.

Comments. An information technology organization recommended adding definitions for registration agent and trusted agent. A security firm suggested the inclusion of several other definitions related to digital signatures.

DEA Response. DEA does not believe that definitions of registration agent and other certification authority terms are needed. DEA has, however, added a definition of "trusted agent," because institutional practitioners may fill this role if they elect to obtain authentication credentials from a certification authority or credential service provider for practitioners using their electronic prescription application to write controlled substances prescriptions. The definition is based on NIST's definition and describes the trusted agent as an entity authorized to act as a representative of a certification authority or credential Service provider in confirming practitioner identification as part of the identity proofing process.[34]

Definition of NIST SP 800-63. In the NPRM, DEA proposed to define the term NIST SP 800-63 as follows: "NIST SP 800-63, as incorporated by reference in § 1311.08 of this chapter, means a Federal standard for electronic authentication." While this term appeared in the definitions, DEA also notes that the Special Publication itself was also proposed to be incorporated by reference in proposed § 1311.08.

[34] National Institute of Standards and Technology. IR-7298 Glossary of Key Information Security Terms, April 25, 2006.

Comments. A healthcare organization stated that the definition of NIST SP 800-63 should be modified to cover future revisions.

DEA Response. DEA has revised the incorporation of NIST SP 800-63 to cover the current version. Federal agencies are not permitted to incorporate by reference future versions of documents.

Definitions of SysTrust and WebTrust. In the NPRM, DEA separately defined the terms SysTrust and WebTrust.

Comments. A healthcare organization believed that SysTrust and WebTrust have converged under the reference of Trust Services for business to business commerce. The commenter believed that a new definition for Trust Services should be introduced and language within the rule modified accordingly for such references.

DEA Response. Although SysTrust and WebTrust are considered part of Trust Services, they are still separate services and identified as such by the American Institute of Certified Public Accountants. Therefore, DEA has not revised these terms in this interim final rule.

Other Definition Issues

Comment. One commenter stated that DEA should adopt the NIST SP 800-63 definition of "possession and control of a token" and recommended that DEA define "sole possession."

DEA Response. DEA does not believe that these definitions are necessary. Both phrases consist of plainly understood terms that have well-established legal meanings.

2. Other Issues

Comments. A number of commenters asked DEA to provide a list of application providers that met DEA's requirements. A practitioner organization, a pharmacy organization, and a physician suggested that DEA make available to prescribers and application providers a database of pharmacies that accept electronic prescriptions. The physician suggested that DEA require all pharmacies to register their ability to accept electronic prescriptions for controlled substances with DEA and for DEA to provide an online automatic directory that enables all electronic health record application providers and electronic prescription application providers to query for all pharmacies and determine immediately if an electronic prescription for a controlled substance can be sent to a particular pharmacy. The commenter suggested that, if it was determined that a particular pharmacy did not accept electronic prescriptions, the electronic health record application or electronic prescription application could then automatically switch to print and notify the prescribing physician of the change and requirement for wet signature and providing the prescription to the patient. This commenter asserted that physicians have had considerable difficulty with the current noncontrolled substance electronic prescribing systems because they could not rely on pharmacy participation or have a reliable means of locating pharmacies. A practitioner organization suggested that DEA could require pharmacies to indicate whether they accept electronic prescriptions as part of DEA's registration process.

DEA Response. DEA does not believe that it is in a position to develop and maintain complete and accurate lists of either application providers that provide applications meeting DEA's requirements for electronic prescriptions for controlled

substances, or of pharmacies that accept electronic prescriptions. Whether an application provider chooses to develop applications that comply with DEA's regulatory requirements and, thus, be in a position to supply applications that may lawfully be used by practitioners to create, sign, and transmit electronic prescriptions for controlled substances and by pharmacies to receive and process electronic prescriptions for controlled substances, is a business decision on the part of that provider. As all providers will be required to undergo third-party audits of their applications, DEA believes that these audit reports, which will be available to interested practitioners, will provide notice of application providers' compliance with DEA regulations. If certification organizations develop programs to certify compliance with DEA's requirements and DEA approves the programs, the certification will also provide practitioners with the information.

Similarly, DEA does not believe it appropriate for DEA itself to maintain a list of pharmacies that accept electronic prescriptions for controlled substances. Again, whether a pharmacy chooses to accept such prescriptions is a business decision left to that pharmacy. DEA is not in a position to proactively and continually monitor pharmacies' involvement in this arena, nor is DEA in a position to continually receive updates from its approximately 65,000 pharmacy registrants regarding their involvement. The electronic prescribing of controlled substances by prescribing practitioners, and the dispensing of those electronic prescriptions by DEA-registered pharmacies, is strictly voluntary. DEA notes that electronic prescription application providers maintain databases of pharmacies that accept electronic prescriptions for routing or other purposes. DEA believes that application providers and/or intermediaries are better suited to the task of maintaining these listings. This is particularly necessary as, due to potential

interoperability issues, a pharmacy that can process prescriptions from one application provider may not be able to process prescriptions from other application providers.

Comments. A number of commenters urged DEA to adopt a particular version of the National Council for Prescription Drug Programs SCRIPT standard and cite particular SCRIPT functions. Several State pharmacist associations asserted that DEA should require the full support of all transaction types of the approved Centers for Medicare and Medicaid Services standards including fill status notification (RXFILL), cancel prescription notification (CANRX) transactions, and prescription change transactions (RXCHG), throughout the prescribing process for controlled substances. The commenters asserted that using these transactions supports medication adherence monitoring and decreases opportunities for diversion. These transactions are already present in the NCPDP SCRIPT standard. A pharmacy Application provider stated that DEA should clarify which SCRIPT transactions must be covered and recommended NEWRX, REFRES, and CHGRES. Pharmacy organizations noted that the SCRIPT standard does not provide explicit standards for some data elements in prescriptions (drug names, dosing, route, and frequency); without standards for these elements, interoperability between pharmacies and practitioners cannot be assured. A pharmacy organization urged DEA to encourage the development of discrete standards for these elements. Practitioner organizations also noted that the SCRIPT standard for sig (directions for use) has not been approved or accepted.

A pharmacy organization stated that it is receiving many reports of errors occurring in electronic prescriptions. The commenter indicated that the prescriptions are quite legible, but, occasionally, quite wrong. Pharmacists are reporting that many

prescriptions are being received by the pharmacy with the drug names and directions for use truncated. In other cases, the directions are incorrect in the space allocated for directions, while the intended instructions are placed in the "comments" section. In other situations, the wrong drug, wrong strength, or totally incorrect directions are transmitted. Occasionally, the quantity of drug is incorrect. There have been a few instances where a computer application, according to anecdotal reports, actually "shuffled" prescriptions in the application, such that the drug intended for one patient appeared on screen for another patient. The organization asserted that errors have been caused by practitioner software and pharmacy software, as well as practitioner keying errors.

DEA Response. DEA shares the concern about prescription errors created by the SCRIPT standard, which is not yet fully functional. DEA, however, does not believe that mandating one version of the standard or particular functions would be useful. The standard continues to evolve; if DEA incorporated by reference one version, it would need to go through rulemaking to update the reference, which could delay implementation of improvements. DEA believes that the best approach is to set minimum requirements to ensure the integrity, authentication, and non-repudiation for controlled substance prescriptions (and in a manner consistent with maintaining effective controls against diversion) and leave the industry to develop all other aspects of electronic prescriptions. This will provide the maximum flexibility while ensuring that DEA's statutory obligations are addressed.

Comments. A few commenters suggested that DEA apply different standards for Schedule II prescriptions. One application provider suggested that Schedule II

prescriptions should remain permissible only as paper prescriptions and that a single-factor authentication protocol be allowed for Schedule III, IV and V prescriptions.

DEA Response. It is true that prescriptions for Schedule II controlled substances are subject to greater statutory and regulatory controls than prescriptions for controlled substances in Schedules III, IV, and V. These differences in controls are commensurate with the differences among these drugs in relative potential for abuse and likelihood of causing dependence when abused. Along similar lines, it is accurate to state that, among the pharmaceutical controlled substances, drugs in Schedule II are subject to the most stringent controls because abuse of these drugs tends to be more harmful to the public health and welfare than abuse of pharmaceutical drugs in lower schedules. Nonetheless, DEA does not believe it is necessary or appropriate to disallow altogether the electronic prescribing of Schedule II controlled substances. Given the carefully crafted requirements contained in this interim final rule, DEA believes that electronic prescribing of all pharmaceutical controlled substances in all schedules can take place without adversely affecting diversion control.

It should also be noted that the required elements of a prescription for a controlled substance (those set forth in 21 CFR 1306.05(a)) are the same for all prescriptions for controlled substances, and this same approach is followed in the interim final rule with respect to electronic prescriptions. Further, DEA believes that disallowing the electronic prescribing of Schedule II controlled substances could significantly hinder adoption of electronic prescribing of controlled substances in other schedules, as it would potentially create separate application requirements for separate schedules, causing confusion among

practitioners, pharmacies, and application providers as to which requirements should be followed for which substances.

Comments. An application provider believed that proposed § 1311.100 is redundant in view of current § 1306.03 and should be deleted.

DEA Response. Current § 1306.03 ("Persons entitled to issue prescriptions.") provides general requirements for the issuance of all prescriptions, written and oral. While the requirements of proposed § 1311.100 (:Eligibility to issue electronic prescriptions.") restated principles from § 1306.03, DEA believes it appropriate to restate those important concepts specifically in regard to electronic prescriptions. Therefore, DEA is retaining the concepts proposed in § 1311.100.

Comments. A healthcare system asked DEA to clarify the specific consequences of non-compliance with each requirement.

DEA Response. The potential consequences of failing to comply with the requirements in this interim final rule regarding the electronic prescribing of controlled substances are the same as the potential consequences of failing to comply with longstanding requirements regarding the general prescribing and dispensing of controlled substances. Just as one cannot list all the potential scenarios in which the existing prescription requirements might be violated, one cannot list all the possible ways in which the various requirements of this interim final rule might be violated. However, as a general matter, if a person fails to comply with the requirements of this interim final rule in a manner that constitutes a criminal or civil violation of the CSA, that person is subject to potential criminal prosecution or civil action as contemplated by the Act. In addition, a DEA registrant who fails to comply with the requirements of the regulations is

subject to potential administrative action that may result in suspension or revocation of his DEA registration.

Comments. A pharmacy organization and an intermediary stated that DEA should revise proposed § 1306.11(a) ("Requirement of prescription [for controlled substances listed in Schedule II].") to read "pursuant to a written or electronic prescription."

DEA Response. DEA has defined paper prescription in § 1300.03. A written prescription includes both paper and electronic prescriptions issued in conformity with the DEA regulations. Thus, the suggested revision is not necessary.

Comments. A number of pharmacist organizations submitted the same comment, listing the following as objectives DEA should pursue in developing the final rule:

- Promoting scalability and nationwide adoption of electronic prescribing by enabling all prescribers, regardless of the volume of controlled substances prescribed, to create and transmit prescriptions for controlled substances via the same electronic media as prescriptions for noncontrolled substances.
- Reducing and eliminating additional costs and administrative burden on pharmacists and prescribers;
- Ensuring compliance and consistency with the uniform standards relating to the requirements for electronic prescription drug programs;
- Improving patient safety and quality of care; and
- Allowing for the expeditious adoption of technological advances and innovation.

DEA Response. DEA has attempted to reduce the burden to practitioners, pharmacies, and others with changes in the interim final rule based on the comments

received, providing flexibility to adopt other technologies as they become feasible, and facilitating adoption of electronic prescriptions for controlled substances. Although admirable goals, uniform standards and improved quality of care are not within DEA's statutory authority; other government agencies are responsible for these issues. DEA recognizes the benefits to pharmacies of uniform standards, but a variety of methods of signing and transmitting electronic prescriptions may satisfy the requirements of the interim final rule and should be allowed for those that wish to use them.

Comments. A number of practitioner organizations urged DEA to ensure that the requirements for electronic prescriptions for controlled substances were cost-effective, particularly for small practices.

DEA Response. DEA believes that the interim final rule will impose even lower costs on registrants than the proposed rule. DEA also notes that the incremental cost of its requirements is relatively small compared to the costs of adopting and installing new applications. A full discussion of the costs and benefits associated with this rule is provided in the required analyses section of this document.

Comments. One advocacy organization asserted that DEA is placing much of the responsibility for application security on practitioners and pharmacies, and asked if DEA has sufficient statutory authority to do so. The commenter asked whether such authority to require this new responsibility lies within the Controlled Substances Act authority to register practitioners.

DEA Response. As set forth at the outset of this preamble, DEA has broad statutory authority under the Controlled Substances Act to issue rules and regulations relating to, among other things, the control of the dispensing of controlled substances,

and to issue and enforce rules and regulations that the agency deems necessary to effectuate the CSA.[35] Also, the structure of the CSA is unlike most statutory schemes in that it prohibits all transactions involving controlled substances except those specifically allowed by the Act and its implementing regulations.[36] The interim final rule is consistent with these aspects of the CSA. It is also worth reiterating here that DEA is not requiring any practitioner to issue electronic prescriptions for controlled substances or any pharmacy to accept them; it is simply setting the requirements that must be met before a practitioner may lawfully issue, and a pharmacy may lawfully process, electronic prescriptions for controlled substances.

As has been discussed previously, nothing in this rule prevents a practitioner or a practitioner's agent from using an existing electronic prescription application that does not comply with the interim final rule to prepare a controlled substance prescription, so that EHR and other electronic prescribing functionality may be used, and print the prescription for manual signature by the practitioner. Such prescriptions are paper prescriptions and subject to the existing requirements for paper prescriptions.

Comments. Some commenters urged DEA to help tighten the security standards imposed under the Health Insurance Portability and Accountability Act. Others cited HIPAA as sufficient to protect the security of electronic prescriptions.

DEA Response. The Department of Health and Human Services is responsible for the HIPAA standards; questions or comments about these standards should be addressed to HHS. The HIPAA security standards are general, leaving many details on

---

[35] 21 U.S.C. 821 & 871(b).
[36] 21 U.S.C. 841(a)(1). See United States v. Moore, 423 U.S. 122, 131 (1975) ("only the lawful acts of registrants are exempted" from the prohibition on distribution and dispensing of controlled substances set forth in 21 U.S.C. 841(a)(1)).

implementation to individual healthcare providers; many of the specifications to implement the security standards are addressable and not mandatory. HIPAA generally focuses on protecting the privacy of the individual patient's information rather than on the possibility of alteration of records or the creation of fraudulent records. As HIPAA was not designed to prevent the diversion of controlled substances, compliance with HIPAA standards alone will not result in the implementation of the types of measures contained in this interim final rule that are specifically tailored to safeguard against diversion.

Comments. A practitioner organization noted that the rule did not specify requirements for what the commenter termed "pharmacy-generated electronic refill requests." The commenter stated that existing electronic prescription applications allow physicians to quickly review and approve electronic refill requests from pharmacies. The commenter asserted that the efficiency of electronic refills is one of the major incentives for physicians to electronically prescribe. The commenter suggested that the final rule should explicitly state whether electronic refill requests will require physicians to take additional steps when authorizing refills of controlled substance prescriptions.

DEA Response. The interim final rule allows for a practitioner to authorize the refilling of an electronic prescription for a controlled substance in the same circumstances that the regulations currently allow a practitioner to authorize the refilling of a paper or oral prescription for a controlled substance. In this context, the following aspects of existing law and regulations should be noted. Part 1306 allows practitioners to authorize refills for controlled substances in Schedules III, IV, and V when the original prescription is written. Schedule II prescriptions may not be refilled, as set forth in the CSA, and

DEA has no authority to depart from that statutory prohibition in the context of paper or electronic prescriptions. If a patient is seeking additional medication not authorized by the original prescription, the practitioner must issue a new prescription regardless of the Schedule. If a pharmacy electronically requests that a practitioner authorize the dispensing of medication not originally authorized on a prescription, or authorize a new prescription based on a previously dispensed prescription, DEA would view any prescriptions issued pursuant to those requests as new prescriptions. If they are written, regardless of whether they are electronic or on paper, they must be signed by the practitioner. Thus, a manual signature would be required for a paper prescription pursuant to § 1306.05, or a practitioner could follow the signature requirements for electronic prescriptions discussed in this rulemaking. Alternatively, for a Schedule III, IV, or V prescription, the pharmacy may receive an oral prescription for that controlled substance, but the pharmacy must immediately reduce that oral, unsigned, prescription to writing pursuant to current regulatory requirements.

Comments. A number of commenters asked that DEA postpone the effective date of the final rule, (i.e., grant what some commenters characterized as an "extended compliance date.") Among these commenters, the range of suggested effective dates was from 18 months to four years after issuance of the final rule.

DEA Response. DEA believes it is unnecessary to postpone the effective date of the interim final rule because use of electronic prescriptions for controlled substances is voluntary. The interim final rule does not mandate that practitioners switch to electronic prescribing of controlled substances. As soon as electronic prescription applications can come into compliance with the requirements of these regulations they may be used for

controlled substance prescriptions. Conversely, practitioners may not use existing electronic prescription applications to transmit electronic prescriptions for controlled substances until those applications are in compliance with the interim final rule. Pharmacy applications may also be used to process electronic prescriptions for controlled substances once they are in compliance with the interim final rule, but not before. DEA notes that existing electronic prescription applications may be used to create a prescription for controlled substances, but until the application is compliant with the rule, that prescription would have to be printed and signed manually, then given to the patient or, for Schedule III, IV, and V prescriptions, faxed to the pharmacy.

Similarly, DEA does not believe it prudent to delay the effective date of this rule for any length of time. DEA wishes to encourage adoption of electronic prescriptions for controlled substances as rapidly as industry is willing and able to comply with the requirements of this rule. DEA recognizes that some health care entities, particularly Federal healthcare facilities, may be more prepared to begin electronically prescribing controlled substances in compliance with this rule than others. To delay the effective date of this rule may unnecessarily hinder those organizations from electronically prescribing controlled substances as quickly as they are able.

Comments. A State pharmacy organization asserted that if it is required to use an intermediary in the transmission of a controlled substance prescription from a practitioner to a pharmacy, the only way to verify a prescription would be to call the practitioner.

DEA Response. DEA does not require the use of any intermediaries in the transmission of electronic prescriptions between prescribing practitioners and pharmacies. There is nothing in the rule that bars the direct transmission of an electronic

prescription from a practitioner to a pharmacy. Until the SCRIPT standard is mature, however, a practitioner whose patients use multiple pharmacies may have to use intermediaries to ensure that the pharmacy will read the data file correctly. DEA believes that the requirements of the interim final rule will provide adequate protections.

Comments. A number of commenters believed that DEA would, could, or should conduct data mining of electronic controlled substance prescriptions. One commenter saw this as a potential threat to civil liberties. Others saw it as a benefit. A pharmacy organization and a chain pharmacy stated that adding requirements for electronic prescriptions will not improve DEA's ability to reduce abuse, but that data mining could. One commenter stated that the benefits to be gained from data mining would allow DEA to impose fewer requirements on electronic prescriptions.

DEA Response. DEA does not conduct a prescription monitoring program (as some States do) or otherwise engage in the generalized collection or analysis of controlled substance prescription data; nor is it the intent of this rule to provide a mechanism for such an activity. The real-time data mining that some commenters feared and others saw as an advantage of electronic prescribing is not contemplated as part of this rulemaking. This rule permits practitioners to write electronic prescriptions for controlled substances and pharmacies to process those electronically written prescriptions. Those applications work independently of DEA and do not directly report prescription information to DEA. This rule merely establishes requirements those applications must meet to be used for electronic prescriptions for controlled substances.

DEA notes that 38 States have implemented prescription monitoring programs that are based on the submission of data from pharmacies after the prescriptions have

been filled. These programs may be used to identify patients who are obtaining prescriptions from multiple practitioners at one time or practitioners who are issuing an unusual number of controlled substance prescriptions.

Comments. A State Board of Pharmacy asserted that there should be a requirement for application integration with all electronic medical record applications and State prescription data banks so that controlled substance prescriptions are readily identifiable.

DEA Response. DEA understands the Board's concern, but believes what the Board seeks is not feasible or appropriate as a DEA regulatory requirement at this time for two reasons. First, electronic prescription applications and electronic health record applications may be installed in many States. Unless all State data banks will be configured in exactly the same way, it would not be possible for an application provider to ensure its application would be integrated with any particular State system. DEA notes that the electronic prescription and electronic health record applications will have to be able to identify controlled substance prescriptions and generate logs of those prescriptions. Second, State systems have generally obtained data from pharmacies rather than practitioners. Pharmacy applications have to be able to identify controlled substance prescriptions.

Comments. A number of commenters representing practitioner organizations and one application provider stated that DEA should not impose any requirements until those requirements have been tested and shown ready for use.

DEA Response. DEA recognizes the value of pilot testing, but does not believe that waiting for pilot testing is necessary or appropriate. Many of the provisions DEA

proposed in its NPRM have been revised based on comments received; DEA has provided options for some key items to give registrants and application providers alternatives. DEA also notes that with so many applications available, what may be feasible for one system may be burdensome for others, so that pilot testing would not necessarily prove whether a particular approach was feasible or difficult for any specific application provider. This is particularly true as electronic prescription applications can be either stand-alone applications or can be integrated into more robust applications, such as electronic health record applications.

Comments. A pharmacy organization asked if the statement in proposed § 1311.200(d) is imposing a strict liability standard.

DEA Response. The statement the commenter references appeared in both proposed § 1311.100(c) ("Eligibility to issue electronic prescriptions.") and proposed § 1311.200(d) ("Eligibility to digitally sign controlled substances prescriptions.") It reads: "The practitioner issuing an electronic controlled substance prescription is responsible if a prescription does not conform in all essential respects to the law and regulations." The statement in proposed § 1311.100(c) and § 1311.200(d) is simply a repetition of the existing requirement in current § 1306.05. This statement has been a part of the regulations implementing the CSA since the regulations were first issued in 1971 following the enactment of the CSA. In the ensuing 38 years, there has never been an occasion in which a court has declared the provision to be legally problematic or in need of elaboration. Accordingly, it is appropriate to retain the concept in the context of electronic prescriptions for controlled substances, which DEA is doing by incorporating the provision in § 1311.100 and § 1311.200.

Comments. Several commenters questioned DEA's concern about diversion. A State Board of Pharmacy asserted that it had found less risk of fraud with electronic prescriptions. Another State Board of Pharmacy disagreed that record integrity was needed to prosecute individuals forging prescriptions, asserting that it did not need to prove when and where a prescription was forged or altered. One physician stated that the problem with diversion was with the patient, not the doctor.

DEA Response. DEA notes that there is no substantial regulatory experience on which State Boards of Pharmacy or other regulating bodies may draw when it comes to electronic prescriptions for controlled substances as such method of prescribing has not, prior to the issuance of this interim final rule, been authorized by the DEA regulations. While there has been electronic prescribing of noncontrolled substances, it is not surprising that there may be little evidence of fraud with prescriptions for such drugs as they are far less likely to be abused and diverted than controlled substances. One State Board of Pharmacy seems to have misunderstood the purpose of the rule or the issues of establishing who altered a prescription when there is no forensic evidence. It is true that with a paper prescription, it may, depending on the circumstances, be unnecessary to establish when and where a prescription was altered because the alteration itself can provide evidence of who did it. With electronic prescriptions, however, there may be no effective means of proving who made the alteration absent evidence of when the change occurred. Likewise, without such evidence, it is difficult, if not impossible, to achieve non-repudiation, and thus the persons actually responsible for the prescription may be able to disclaim responsibility. As for the practitioner commenter who attributed the problem to the patient, DEA agrees that patients can be sources of diversion of controlled

substances, but a considerable amount of diversion also occurs from within practitioners' offices and pharmacies as well.

Comments. One application provider stated that the evidence that DEA presented on insider threats in the NPRM would not have been available if these threats had not been identified. The commenter asserted that the ability of the Secret Service/Carnegie Mellon study[37] to identify the character of the employees as well as their "technical" status indicates that existing industry standards are sufficient to detect and investigate the nature of violations.

DEA Response. That studies have been able to identify the kinds of people who commit insider crimes does not support an argument that insider crimes are, therefore, not a problem or are easily identified or prosecuted. Further, most of the insider attacks mentioned in the study to which this commenter referred were identified because the insiders or former insiders intended the attack to be obvious and destructive; these were usually revenge attacks by disgruntled employees or former employees. With financial insider attacks, the victim has reason to identify the attack because the attack results in financial losses. If insider attacks occur with electronic prescription applications, the application providers will not be the target or suffer financial losses; their applications will simply be used to commit a crime. In any event, regardless of what studies might purport to show with respect to insider attacks of computer-based systems, DEA has an obligation in this rulemaking to establish requirements that are particularly crafted to maintain effective controls against diversion of controlled substances in the context of

[37] Insider Threat Study: Illicit Cyber Activity in the Banking and Financial Sector, August 2004; Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, May 2005

electronic prescribing. DEA is aware of no study that refutes DEA's determination about the need for the controls contained in this interim final rule.

Comments. One commenter, a physician, suggested that DEA and the Centers for Medicare and Medicaid Services go back to the electronic prescribing and electronic health record industries and tell them to incorporate DEA's proposed system upgrades, that these be operational in any CCHIT-approved system before moving ahead with these standards, and that DEA tell Congress that no penalties should be applied to any non-adopting physician before the system has been upgraded to the satisfaction of DEA.

DEA Response. Consistent with the Administrative Procedure Act, DEA will articulate through this interim final rule those regulatory requirements regarding electronic prescriptions for controlled substances. DEA does not believe it would be legally sound or consistent with the public health and safety to declare that physicians or any other persons may disregard, without legal consequence, the standards established by this interim final rule.

Comment. A State said that checks for the validity and completeness of a prescription should occur at the prescriber's office. A pharmacy employee stated that prescribers should not be able to transmit prescriptions unless the prescription meets all regulations of the State where the prescription will be filled. This individual further believed that prescriptions should be allowed to be filled anywhere in the country. Finally, this individual recommended that there be provisions to permit the transfer of the prescription to another pharmacy even if it is out of State.

DEA Response. Section 1306.05 states that the practitioner is responsible for ensuring that a prescription conforms in all essential respects with the law and regulation;

it also places a corresponding liability on pharmacies to ensure that only prescriptions that conform with the regulations are dispensed. The interim final rule requires that the electronic prescription application be capable of capturing all of the information and that the practitioner review the prescription before signing it. This requirement, however, does not relieve a pharmacy of its responsibility to ensure that the prescription it receives conforms to the law and regulations.

As this interim final rule is a DEA rule, it is, of course, focused on Federal, not State, requirements. In view of this comment, however, it should be noted that the CSA has long provided that a practitioner who fails to comply with applicable State laws relating to controlled substances is subject to loss of DEA registration.[38] Similarly, it has always been the case that compliance with the CSA or DEA regulations does not relieve anyone of the additional obligation to comply with any State requirements that pertain to the same activity.[39] Thus, it is both the practitioner's and the pharmacy's responsibility to ensure that the prescription complies with all applicable laws and regulations. DEA does not limit where a prescription may be filled, nor does it limit where a prescription may be transferred, provided such transfers take place in a manner authorized by the DEA regulations.

3. Beyond the Scope

A number of commenters raised issues that are beyond the scope of this rulemaking (e.g., requirements on the number of registrations that a practitioner must hold, penalties and incentives for electronic prescribing, the inability to set an indefinite quantity in prescriptions for LTCF patients). Consistent with sound APA practice, and to

[38] 21 U.S.C. 823(f)(4).
[39] See 21 U.S.C. 903.

avoid unnecessary discussion, DEA will not address in this interim final rule such comments that are not directly related to the electronic prescribing of controlled substances.

L. Summary of Changes from the Proposed Rule

In view of the comments that DEA received, the interim final rule contains a number of changes to the proposed rule. For the most part, the changes are logical outgrowths of the proposed rule and comments. In some instances, however, DEA has determined that the changes from the proposed rule warrant additional public comment. To assist the reader in understanding the changes, this section summarizes the major revisions. Commenters made a variety of recommendations on each issue. Where DEA determined that it could accept recommendations without lessening the security and integrity of controlled substance prescriptions, it has done so to provide more flexibility and lessen the burden on practitioners and pharmacies.

Identity proofing. DEA has adopted in the interim final rule an approach that is different from the approach it proposed. As some commenters recommended, the interim final rule requires individual practitioners to obtain NIST SP 800-63-1 Assurance Level 3 identity proofing from entities that are Federally approved to conduct such identity proofing; NIST SP 800-63-1 Assurance Level 3 allows either in-person or remote identity proofing, subject to the NIST requirements. The Federally approved entities will provide the two-factor authentication credentials for individual practitioners. As commenters suggested, institutional practitioners have the option to conduct identity proofing in-house through their credentialing offices and may issue the two-factor authentication credentials themselves.

Access control. In contrast to the proposed rule, the interim final rule places the responsibility for checking the DEA and State authorities and setting logical access on the individual practice or institution rather than on the application provider. Commenters indicated that many application providers were not involved in these actions. Under the interim final rule, two individuals are required to enter or change logical access controls. The applications must limit access for indicating that a controlled substance prescription is ready for signing and signing to individuals authorized under DEA regulations to do so.

Two-factor authentication. The interim final rule retains the proposed requirement of two-factor authentication, but as commenters requested, allows the option of using a biometric to replace the hard token or the knowledge factor. DEA has also revised the rule to allow the hard token, when used, to be compliant with FIPS 140-2 Security Level 1 or higher, provided that the token is separate from the computer being accessed. DEA has revised the rule to allow practitioners with multiple DEA numbers to use a single two-factor authentication credential per practitioner; the application must require these practitioners to select the appropriate DEA number for the prescription being issued. As commenters requested, the interim final rule also includes an application requirement that will allow a supervisor's DEA number to appear on the prescription provided it is clear which DEA number is associated with the prescribing practitioner.

Creating the prescription. As proposed, the interim final rule requires that practitioners indicate that each controlled substance prescription is ready to be signed. As commenters recommended, however, the patient's address need not appear on the

review screen, but it must still be included on the transmitted prescription, consistent with longstanding regulations applicable to all prescriptions for controlled substances. The proposed attestation statement has been shortened and must appear on the screen at the time of the review, but, as some commenters recommended, does not require a separate keystroke. Also under the interim final rule, authentication to the application must occur at signing, eliminating the need for the proposed lock-out provision.

Signing and transmitting the prescription. As some commenters recommended, the interim final rule requires two-factor authentication to be synonymous with signing. In fact, the interim final rule expressly states that the completion of the two-factor authentication protocol by the practitioner legally constitutes that practitioner's signature of the prescription. When the practitioner completes the two-factor authentication protocol, the application must apply its (or the practitioner's) private key to digitally sign at least the information required under part 1306. That digitally signed record must be electronically archived. As commenters suggested, this revision allows other staff members to add information not required by DEA regulations after signature, such as pharmacy URLs, and at LTCFs, allows staff to review and annotate records before transmission, so that current workflows can be maintained. The interim final rule retains the proposed requirement that the electronic prescription application include an indication that the prescription was signed in the information transmitted to the pharmacy.

PKI. At the suggestion of many commenters, the interim final rule allows any practitioner to use the digital signature option proposed for Federal healthcare systems.

Transmission issues. The interim final rule adopts the suggestion of some commenters that printing of a transmitted electronic prescription be permissible provided

the printed prescription is clearly marked as a copy not for dispensing. The interim final rule specifies the conditions for printing a prescription when transmission fails, as commenters asked. DEA has also clarified in the interim final rule that the prohibition on alteration of content during transmission applies to the actions of intermediaries; changes made by pharmacies are subject to the same rules that apply to all prescriptions for controlled substances. As proposed, intermediaries are not allowed under the interim final rule to transform an electronic prescription into a facsimile; facsimiles of prescriptions are paper prescriptions that must be manually signed.

Monthly logs. As some commenters recommended, DEA has retained in the interim final rule the requirement that the application automatically provide the practitioner with a monthly log of the practitioner's electronic prescribing of controlled substances. However, the interim final rule eliminates the proposed requirement that the practitioner indicate his review of the log. DEA has also maintained in the interim final rule the proposed requirement that the application provide practitioners a log on request. The interim final rule goes somewhat further than the proposed rule in this respect by requiring that the application allow the practitioner to specify the time period for log review, and to allow the practitioner to request and obtain a display of up to a minimum of two years of prior electronic prescribing of controlled substances and to request a display for particular patients or drugs.

Internal audit trails. DEA has provided in the interim final rule more detail on the requirements for the internal audit trails required for both prescription and pharmacy applications. The interim final rule does not provide a comprehensive list of auditable events as some commenters requested, but clarifies that auditable events should be

limited to potential security problems. For pharmacy applications, the interim final rule eliminates the proposed requirement that the audit trail log each time a prescription is opened, as commenters suggested.

Other pharmacy issues. DEA has retained in the interim final rule the proposed requirement that either the last intermediary or the pharmacy digitally sign the prescription as received unless a practitioner's digital signature is attached and can be verified by the pharmacy. However, as commenters suggested, the interim final rule revises the requirement for checking the DEA registration of the practitioner to make it consistent with other prescriptions: the pharmacy must check the DEA registration when it has reason to suspect the validity of the registration or the prescription. Although DEA recommends as a best practice offsite storage of backup copies, it is not requiring it in the interim final rule as was proposed.

Third-party audits. As commenters recommended, the interim final rule allows certification of electronic prescription applications and pharmacy applications by a DEA-approved certification organization to replace a third-party audit. The interim final rule also expands beyond the proposed rule the list of potential auditors to include certified information system auditors. As commenters suggested, the interim final rule extends the time frame for periodic audits from one year to two years, or whenever a functionality related to controlled substance prescriptions is altered, whichever occurred first.

Recordkeeping. Based on the comments received, the interim final rule reduces the recordkeeping period to two years from the proposed five years.

DEA wishes to emphasize that the electronic prescribing of controlled substances is in addition to, not a replacement of, existing requirements for written and oral

prescriptions for controlled substances. This rule provides a new option to prescribing practitioners and pharmacies. It does not change existing regulatory requirements for written and oral prescriptions for controlled substances. Prescribing practitioners will still be able to write, and manually sign, prescriptions for Schedule II, III, IV, and V controlled substances, and pharmacies will still be able to dispense controlled substances based on those written prescriptions and archive those records of dispensing. Further, nothing in this rule prevents a practitioner or a practitioner's agent from using an existing electronic prescription application that does not comply with the interim final rule to prepare a controlled substance prescription electronically, so that EHR and other electronic prescribing functionality may be used, and print the prescription for manual signature by the practitioner. Such prescriptions are paper prescriptions and subject to the existing requirements for paper prescriptions.

V. Section-by-Section Discussion of the Interim Final Rule

In Part 1300, DEA is adding a new § 1300.03 ("Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.") The definitions currently in § 1311.02 are moved to § 1300.03. Definitions of the following are established without revision from the NPRM: "audit trail," "authentication," "electronic prescription," "identity proofing," "intermediary," "paper prescription," "PDA," "SAS 70," "SysTrust," "token," "valid prescription," and "WebTrust." Based on comments received, DEA is establishing the definition of "hard token," with changes as discussed above. Based on comments received, DEA is adding definitions of the terms "application service provider," "electronic prescription application provider," "installed electronic prescription application," "installed pharmacy

application," "pharmacy application provider," and "signing function." DEA is updating the proposed definition of "NIST SP 800-63" to reflect the most current version of this document.

Other changes to definitions. Beyond the revisions discussed above, DEA has made several changes to the definitions section established in this rulemaking. Although not specifically discussed by commenters, DEA has made other changes to certain definitions to provide greater clarity, specificity, or precision. Changes are discussed below.

To address the use of a biometric as one possible factor in a two-factor authentication credential, DEA is adding definitions specific to that subject. Specifically, DEA is adding definitions of "biometric subsystem," "false match rate," "false non-match rate," "NIST SP 800-76-1," and "operating point." While DEA is adding a definition of "password" to mean "a secret, typically a character string (letters, numbers, and other symbols), that a person memorizes and uses to authenticate his identity," DEA is not establishing any regulations regarding password strength, length, format, or character usage.

In the definition of authentication protocol, DEA revised the language slightly to read: "Authentication protocol means a well specified message exchange process that verifies possession of a token to remotely authenticate a person to an application." The proposed language had read "to remotely authenticate a prescriber."

As discussed elsewhere in this rule, DEA is revising certain recordkeeping requirements. To ensure that terms used regarding recordkeeping are understood, DEA has repeated the definition of "readily retrievable" from 21 CFR 1300.01(b)(38). This

definition is longstanding and is well understood by the regulated industry. DEA does not believe that this definition will cause the regulated industry any difficulty. Since the inception of the CSA, the DEA regulations have defined the term as follows: "Readily retrievable means that certain records are kept by automatic data processing systems or other electronic or mechanized recordkeeping systems in such a manner that they can be separated out from all other records in a reasonable time and/or records are kept on which certain items are asterisked, redlined, or in some other manner visually identifiable apart from other items appearing on the records."

In its NPRM, DEA proposed to define the term "audit" as follows: "audit means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures." To provide greater specificity to this term, DEA has revised the term to be "third-party audit" rather than simply "audit." The definition remains unchanged from the NPRM in all other respects.

DEA has added definitions of credential and credential service provider based on the NIST definitions in NIST SP 800-63-1.

DEA has added definitions for the updated NIST FIPS standards. Finally, DEA is defining the term "trusted agent" to provide greater specificity regarding identity proofing conducted by institutional practitioners.

In Part 1304, § 1304.04 is revised to limit records that cannot be maintained at a central location to paper order forms for Schedule I and II controlled substances and paper prescriptions. In paragraph (b)(1), DEA is removing the reference to prescriptions;

all prescription requirements are moved to paragraph (h). Paragraph (h), which details pharmacy recordkeeping, is revised to limit the current requirements to paper prescriptions and to state that electronic prescriptions must be retrievable by prescriber's name, patient name, drug dispensed, and date filled. The electronic records must be in a format that will allow DEA or other law enforcement agencies to read the records and manipulate them; preferably the data should be downloadable to a spreadsheet or database format that allows DEA to sort the data. The data extracted should only include the items DEA requires on a prescription. Records are required to be capable of being printed upon request.

DEA is adding a new § 1304.06 ("Records and reports for electronic prescriptions.") This section does not create new recordkeeping requirements, but rather simply consolidates and references in one section requirements that exist in other parts of the rule. This new section is intended to make it easier for registrants and application providers to understand the records and reports they are required to maintain. Practitioners who issue electronic prescriptions for controlled substances must use electronic prescription applications that retain the record of the digitally signed prescription information and the internal audit trail and any auditable event identified by the internal audit trail. Institutional practitioners must retain a record of identity proofing and issuance of the two-factor authentication credential, where applicable, as required by § 1311.110. Pharmacies that process electronic prescriptions for controlled substances must use a pharmacy application that retains all prescription and dispensing information required by DEA regulations, the digitally signed record of the prescription as received by the pharmacy, and the internal audit trail and any auditable event identified by the

internal audit trail. Registrants and application service providers must retain a copy of any security incident report filed with the Administration. Application providers must retain third-party audit or certification reports and any adverse audit or certification reports filed with the Administration regarding problems identified by the third-party audit or certification. All records must be retained for two years unless otherwise specified. DEA is not establishing any recordkeeping requirements for credential service providers or certification authorities because they are already subject to such requirements under the terms of certificate policies or frameworks they must meet to gain Federal approval.

In Part 1306 ("Prescriptions") § 1306.05 is amended to state that electronic prescriptions must be created and signed using an application that meets the requirements of part 1311 and to limit some requirements to paper prescriptions (e.g., the requirement that paper prescriptions have the practitioner's name stamped or hand-printed on the prescriptions). The section also adds "computer printer" to the list of methods for creating a paper prescription and clarifies that a computer-generated prescription that is printed out or faxed must be manually signed. DEA is aware that in some cases, an intermediary transferring an electronic prescription to a pharmacy may convert a prescription to a facsimile if the intermediary cannot complete the transmission electronically. As discussed previously in this rule, for controlled substance prescriptions, transformation to facsimile by an intermediary is not an acceptable solution. The section, as proposed, is also revised to divide paragraph (a) into shorter units.

Section 1306.08 is added to state that practitioners may sign and transmit controlled substance prescriptions electronically if the applications used are in compliance with part 1311 and all other requirements of part 1306 are met. Pharmacies are allowed to handle electronic prescriptions if the pharmacy application complies with part 1311 and the pharmacy meets all other applicable requirements of parts 1306 and 1311.

As proposed, §§ 1306.11, 1306.13, and 1306.15 are revised to clarify how the requirements for Schedule II prescriptions apply to electronic prescriptions.

As proposed, § 1306.21 is revised to clarify how the requirements for Schedule III, IV, and V prescriptions apply to electronic prescriptions.

As proposed, § 1306.22 is revised to clarify how the requirements for Schedule III and IV refills apply to electronic prescriptions and to clarify that requirements for electronic refill records for paper, fax, or oral prescriptions do not apply to electronic refill records for electronic prescriptions. Pharmacy applications used to process and retain electronic controlled substance prescriptions are required to comply with the requirements in part 1311. In addition, DEA is breaking up the text of the existing section into shorter paragraphs to make it easier to read.

As proposed, § 1306.25 is revised to include separate requirements for transfers of electronic prescriptions. These revisions are needed because an electronic prescription could be transferred without a telephone call between pharmacists. Consequently, the transferring pharmacist must provide, with the electronic transfer, the information that the recipient transcribes when accepting an oral transfer. DEA notes that the NPRM contained language proposing to permit an electronic prescription to be transferred more

than once, in conflict with the requirements for paper and oral prescriptions. DEA has removed this proposed requirement; all transfer requirements for electronic prescriptions are consistent with those for paper and oral prescriptions.

Finally, DEA notes that it had proposed a new § 1306.28 to state the basic recordkeeping requirements for pharmacies for all controlled substance prescriptions. Those requirements are present in § 1304.22. Although DEA initially believed that including these requirements in part 1306 would be beneficial, after further consideration DEA believes that they would be redundant and could, in fact, create confusion. Therefore, DEA is not finalizing proposed 21 CFR 1306.28.

DEA is revising the title of part 1311 as proposed.

Section 1311.08 is revised to include the incorporations by reference of FIPS 180-3, Secure Hash Standard; FIPS 186-3, Digital Signature Standard; and NIST SP 800-63-1 Draft Electronic Authentication Guideline.

Subpart C is being added by this interim final rule. DEA has revised the content of proposed subpart C, as discussed above, and has reorganized the subpart. The following describes each of the sections in the interim final subpart C.

Section 1311.100 provides the general requirements for issuing electronic controlled substance prescriptions. It clarifies that the rules apply to all controlled substance prescriptions; the same electronic prescription requirements apply to Schedule II prescriptions as apply to other controlled substance prescriptions. DEA notes that the statutory prohibition on refilling Schedule II prescriptions remains in effect regardless of whether the prescription is issued electronically or on paper (21 U.S.C. 829(a), 21 CFR 1306.12(a)). Only a practitioner registered or exempt from registration and

authorized to issue the prescription may do so; the prescription must be created on an application that meets all of the requirements of part 1311 subpart C. A prescription is not valid if the application does not meet the requirements of the subpart or if any of the required application functions were disabled when it was created. A pharmacy may process electronic controlled substance prescriptions only if its application meets the requirements of the subpart.

Section 1311.102 specifies the practitioner's responsibilities. A practitioner must retain sole control of the hard token, where applicable, and must not share the password or other knowledge factor or biometric information. The practitioner must notify the individuals designated to set logical access controls within one business day if the hard token has been lost, stolen, or compromised, or the authentication protocol has otherwise been compromised.

If the practitioner is notified by an intermediary or pharmacy that an electronic prescription was not successfully delivered, he must ensure that any paper or oral prescription (where permitted) issued as a replacement of the original electronic prescription indicates that the prescription was originally transmitted electronically to a particular pharmacy and that the transmission failed.

As discussed previously, if the third-party auditor or certification organization finds that an electronic prescription application does not accurately and consistently record, store, and transmit the information related to the name, address, and registration number of the practitioner, patient name and address, and prescription information (drug name, strength, quantity, directions for use), the indication of signing, and the number of

refills, the practitioner must not use the application to sign and transmit electronic prescriptions for the controlled substances.

Further, if the third-party auditor or certification organization finds that an electronic prescription application does not accurately and consistently record, store, and transmit other information required for prescriptions, the practitioner must not sign and transmit electronic prescriptions for controlled substances that are subject to the additional information requirements.

In most cases, this will not be an issue as the SCRIPT standard supports the standard information required for a prescription. A limited number of prescriptions, however, require special information. Prescriptions for GHB require a note on medical need; prescriptions for drugs used for detoxification and maintenance treatment require an additional DEA identification number. Schedule II prescriptions may be issued with written instructions indicating the earliest date that the prescription may be filled. DEA is not certain that the existing SCRIPT standard accommodates the additional information or that existing pharmacy applications accurately and consistently capture and display such information. Because there are relatively few prescriptions with these requirements, DEA decided to place the onus on the third-party auditors or certification organizations to determine whether applications can create, transmit, import, display, and store all of the information needed for these prescriptions. If an electronic prescription application does not allow the entry of this additional information, the practitioner must not issue the prescriptions electronically. DEA decided that this approach was preferable to making it an application requirement that all applications would have to meet before they could be used to issue or process any controlled substance prescriptions electronically. DEA

believes that there may be a difference between adding a single-character field to the SCRIPT standard, indicating that the prescription was signed, which would be transmitted with almost all prescriptions, and adding a set of additional fields, some of which could be defined in multiple ways. For example, future fill dates could be placed in fields defined as future fill dates and presented as dates or they could be presented as text. NCPDP may need time to decide how to add fields to capture this information; application providers cannot begin to reprogram until decisions on the standard are reached. DEA does not believe it is necessary or appropriate to delay adoption of electronic controlled substance prescriptions until these issues are resolved.

Section 1311.102 also states that a practitioner must not use the application for controlled substance prescriptions if any of the functions have been disabled or is not working properly. Finally, if the application provider notifies him that the third-party audit indicated that the application does not meet the requirements of part 1311, or that the application provider has identified a problem that makes the application non-compliant, the practitioner must immediately cease to issue controlled substance prescriptions using the application and must ensure that access for signing controlled substance prescriptions is terminated. The practitioner must not use the application to issue controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

Sections 1311.105 and 1311.110 specify the requirements for obtaining an authentication credential for individual practitioners and practitioners using an institutional practitioner's application, as discussed above.

Section 1311.115 specifies the requirements for two-factor authentication. It allows the authentication protocol to use any two of the three authentication factors (something you know, something you are, and something you have) and sets the requirements that hard tokens must meet.

Section 1311.116 specifies the requirements that biometric subsystems must meet.

Section 1311.120 provides the electronic prescription application requirements.

Section 1311.120(b)(1) requires an electronic prescription application to link each registrant, by name, with a DEA registration number. For practitioners exempt from the requirement of registration under § 1301.22(c), the application must link each practitioner to the institutional practitioner's DEA registration number and the specific internal code number required under § 1301.22(c)(5).

Section 1311.120(b)(2) requires an electronic prescription application to allow setting of logical access controls for indicating that prescriptions are ready to be signed and signing controlled substance prescriptions. It also requires the application to allow the setting and changing of logical access controls.

Section 1311.120(b)(3) states that logical access controls must be set by user name or role. If the application uses role-based access controls, it must not allow an individual to be assigned the role of registrant unless the individual is linked to a DEA registration number.

Section 1311.120(b)(4) requires that setting and changing of logical access controls must take the actions of two individuals, as discussed above.

Section 1311.120(b)(5) states that the application must accept two-factor authentication credentials and require their use for approving logical access controls and signing prescriptions.

Section 1311.120(b)(6) states that an electronic controlled substance prescription must contain all of the information required under part 1306. As commenters pointed out, although the SCRIPT standard has fields for most of this information, the use of these fields is not always mandated. Some of the required information may have to be put in free text fields (e.g., internal institutional code data or service identification numbers for practitioners exempt from registration, the medical need for GHB prescriptions, a separate identification number for certain prescriptions).

Section 1311.120(b)(7) states that the application must require the practitioner or his agent to select the DEA number to be used for the prescription where the practitioner issues prescriptions under more than one DEA number. This provision is intended to prevent the application from automatically filling in the DEA number field when a practitioner uses more than one number.

Section 1311.120(b)(8) states that the electronic prescription application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

Section 1311.120(b)(9) specifies the information that must appear on the review screen. As explained above, if a practitioner has written several prescriptions for a single patient, the practitioner's and patient's information may appear only once on the review screen.

Section 1311.120(b)(10) states that the application must require the practitioner to indicate that each controlled substance prescription is ready for signing. If any of the information required under part 1306 is altered after the practitioner has indicated that it is ready for signing, the application must remove the indication that it is ready for signing and require another indication before allowing it to be signed. The application must not allow the signing or transmission of a prescription that was not indicated as ready to be signed.

Section 1311.120(b)(11) provides the requirement that the practitioner use the two-factor authentication protocol to sign the prescription.

Section 1311.120(b)(12) states that the application must not allow a practitioner to sign a prescription if his two-factor authentication credential is not associated with the prescribing practitioner's DEA number listed on the prescription (or an institutional practitioner's DEA number and the prescriber's extension data). The application will have to associate each two-factor authentication credential with the registrant's DEA number(s) (or institutional practitioner's DEA number plus the individual practitioner's extension data) and ensure that only the authentication credentials associated with the number on the prescription can indicate the prescription as ready for signing and sign it. This provision is needed to prevent one registrant in a practice from reviewing and signing prescriptions written by other registrants. DEA recognizes that with paper prescriptions, DEA numbers for every member of a practice may be printed on a prescription pad; only the signature indicates which practitioner issued the prescription. For electronic prescriptions, however, only one prescribing practitioner's name will appear and one DEA number. Although the authentication credential will be associated

with only one practitioner, it may be associated with more than one DEA number. If a practitioner needs to sign a prescription originally created and indicated as ready for signing by another practitioner in a practice, he must change the practitioner name and DEA number to his own, then indicate that the prescription is ready to sign and execute the two-factor authentication protocol to sign it.

Section 1311.120(b)(13) states that where a practitioner seeks to prescribe more than one controlled substance at one time for a particular patient, the electronic prescription application may allow the practitioner to sign multiple prescriptions for a single patient at one time using a single invocation of the two-factor authentication protocol provided that the practitioner has individually indicated that each controlled substance prescription is ready to be signed while all the prescription information and the statement described in § 1311.140 are displayed.

Section 1311.120(b)(14) states that the application must time and date stamp the prescription on signing.

Section 1311.120(b)(15) states that when the practitioner executes the two-factor authentication protocol, the application must digitally sign and electronically archive at least the information required by DEA. If the practitioner is signing the prescription with his own private key, the application must electronically archive the digitally signed prescription, but need not digitally sign the prescription a second time.

Section 1311.120(b)(16) specifies the requirements for a digital signature. The cryptographic module must be validated at FIPS 140-2 Security Level 1. The digital signature application and hash function must comply with FIPS 186-3 and FIPS 180-3. The electronic prescription application's private key must be stored encrypted on a FIPS

140-2 Security Level 1 validated cryptographic module using a FIPS-approved encryption algorithm. For software implementations, when the signing module is deactivated, the application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

Section 1311.120(b)(17) states that the prescription transmitted to the pharmacy must include an indication that the prescription was signed unless the prescription is being transmitted with the practitioner's digital signature.

Section 1311.120(b)(18) states that a prescription must not be transmitted unless the signing function was used.

Section 1311.120(b)(19) states that the information required under part 1306 must not be altered after the prescription is digitally signed. If any of the required information is altered, the prescription must be canceled.

Section 1311.120(b)(20) through (22) specify the requirements for printing transmitted prescriptions.

Section 1311.120(b)(23) states that the application must maintain an audit trail related to the following: the creation, alteration, indication of readiness for signing, signing, transmission, or deletion of a controlled substance prescription; the setting or changing of logical access controls related to controlled substance prescriptions; and any notification of failed transmission. Section 1311.120(b)(24) specifies the information that must be maintained in the audit trail: date and time of the action, type of action, identity of the person taking the action, and outcome.

Section 1311.120(b)(25) states that the application must be capable of conducting an internal audit and generating a report on auditable events.

Section 1311.120(b)(26) states that the application must protect audit trail records from unauthorized deletion, and must prevent modifications to the records.

Section 1311.120(b)(27) specifies the requirements for the monthly log.

Section 1311.120(b)(28) specifies that all records that the application is required to generate and archive must be retained electronically for at least two years.

Sections 1311.125 and 1311.130 specify the requirements for setting and changing logical access controls at an individual practitioner's practice and at an institutional practitioner, respectively.

Section 1311.135 sets the basic application requirements for creating an electronic controlled substance prescription. It states that either a practitioner or his agent may enter prescription information. If a DEA registrant holds more than one registration that he uses to issue prescriptions, the application must require him to select the registration number for each prescription. The application cannot set a default or pre-fill the field if the practitioner has more than one registration. If a practitioner has only one registration, as most practitioners do, the application could automatically fill that field. If required by State law, a supervisor's name and DEA number may be listed on a prescription, provided the prescription clearly indicates who is the supervisor and who is the prescribing practitioner.

Section 1311.140 provides the application requirements for signing an electronic prescription for a controlled substance. It requires that the screen displaying the prescription information for review include the statement that completing the two-factor authentication protocol signs the prescription and that only the practitioner whose name and DEA number are on the prescription may sign it. After the practitioner has indicated

that one or more controlled substance prescriptions for a single patient are ready for signing, the application must prompt the practitioner to execute the two-factor authentication protocol. The completion of the two-factor authentication protocol must apply the application's (or practitioner's) digital signature to the DEA-required information and electronically archive the digitally signed record. The application must clearly label as the signing function the function that applies the digital signature. Any controlled substance prescription not signed in this manner must not be transmitted.

Section 1311.145 specifies the requirements for the use of a practitioner's digital certificate and the associated private key. The digital certificate must have been obtained in accordance with the requirements of § 1311.105. The digitally signed record must be electronically archived. The section specifies that if the prescription is transmitted without the digital signature attached, the application must check the Certificate Revocation List to ensure that the certificate is valid and must not transmit the prescription if the certificate has expired. The section also clarifies that if a practitioner uses his own private key, the application need not apply its private key to sign the record.

Section 1311.150 specifies the requirements for auditable events for electronic prescription applications. Auditable events must include at least the following: attempted or successful unauthorized access to the application; attempted or successful unauthorized deletion or modification of any records required by part 1311; interference with application operations related to prescriptions; any setting of or changes to logical access controls related to controlled substance prescriptions; attempted or successful interference with audit trail functions; and, for application service providers, attempted or successful creation, modification, or destruction of controlled substance prescriptions or

logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider. The application must run the internal audit once every calendar day and generate a report that identifies any auditable event. This report must be reviewed by an individual authorized to set access controls. If the auditable event compromised or could have compromised the integrity of the records, this must be reported to DEA and the application provider within one business day of discovery.

Section 1311.170 requires that the application transmit the prescription as soon as possible after signature by the practitioner. The section requires that the electronic prescription application not allow the printing of an electronic prescription that has been transmitted unless the pharmacy or intermediary notifies the practitioner that the electronic prescription could not be delivered to the pharmacy designated as the recipient or was otherwise rejected. If a practitioner is notified that an electronic prescription was not successfully delivered to the designated pharmacy, the application may print the prescription for the practitioner's manual signature. The prescription must include information noting that the prescription was originally transmitted electronically to [name of specific pharmacy] on [date/time], and that transmission failed.

The section indicates that the application may print copies of the transmitted prescription if they are clearly labeled as copies not valid for dispensing. Data on the prescription may be electronically transferred to medical records and a list of prescriptions written may be printed for patients if the list indicates that it is for informational purposes only. The section clarifies that the electronic prescription

application must not allow the transmission of an electronic prescription if a prescription was printed for signature prior to attempted transmission.

Finally, the section specifies that the contents of the prescription required under part 1306 must not be altered during transmission between the practitioner and pharmacy. Any change to this required content during transmission, including truncation or removal of data, will render the prescription invalid. The contents may be converted from one software version to another; conversion includes altering the structure of fields or machine language so that the receiving pharmacy application can read the prescription and import the data into its application. At no time may an intermediary convert an electronic controlled substance prescription data file to another form (e.g., facsimile) for transmission.

Section 1311.200 specifies the pharmacy's responsibility to process controlled substance electronic prescriptions only if the application meets the requirements of part 1311. The section also requires the pharmacy to determine which employees may access functions for annotating, altering, and deleting prescription information (to the extent such alteration is permitted by the CSA and its implementing regulations) and for implementing those logical access controls. As discussed previously, if the third-party auditor or certification organization finds that a pharmacy application does not accurately and consistently import, store, and display the information related to the name, address, and registration number of the practitioner, patient name and address, and prescription information (drug name, strength, quantity, directions for use), the indication of signing, and the number of refills, the pharmacy must not accept electronic prescriptions for the controlled substance. If the third-party auditor or certification organization finds that a

pharmacy application does not accurately and consistently import, store, and display other information required for prescriptions, the pharmacy must not accept electronic prescriptions for controlled substances that are subject to the additional information requirements.

The section specifies that if a prescription is received electronically, all annotations and recordkeeping related to that prescription must be retained electronically. The section reiterates the responsibility of the pharmacy to dispense controlled substances only in response to legitimate prescriptions.

Section 1311.205 provides the requirements for pharmacy applications.

Section 1311.205(b)(1) states that the application must allow the pharmacy to set access controls to limit access to functions that annotate, alter, or delete prescription information, and to the setting or changing of logical access controls.

Section 1311.205(b)(2) states that logical access controls must be set by name or role.

Section 1311.205(b)(3) specifies that the application must digitally sign and archive an electronic prescription upon receipt or be capable of receiving and archiving a digitally signed record.

Section 1311.205(b)(4) specifies the requirements for the digital signature functionality for pharmacy applications that digitally sign prescription records upon receipt.

Section 1311.205(b)(5) states that the pharmacy application must validate a practitioner's digital signature if the pharmacy accepts prescriptions digitally signed by the practitioner and transmitted with the digital signature.

Section 1311.205(b)(6) states that if a practitioner's digital signature is not sent with the prescription, either the application must check for the indication that the prescription was signed or the application must display the indication for the pharmacist to check.

Section 1311.205(b)(7) states that the application must read and retain the entire DEA number including the specific internal code number assigned to an individual practitioner prescribing controlled substances using the registration of the institutional practitioner.

Section 1311.205(b)(8) states that the application must read and store, and be capable of displaying, all of the prescription information required under part 1306.

Section 1311.205(b)(9) states that the pharmacy application must read and store in full the information required under § 1306.05(a). Either the pharmacist or the application must verify all the information is present.

Section 1311.205(b)(10) states that the application must allow the pharmacy to add information on the number/volume of the drug dispensed, the date dispensed, and the name of the dispenser.

Section 1311.205(b)(11) specifies that the application must be capable of retrieving prescription information by practitioner name, patient name, drug name, and date dispensed.

Section 1311.205(b)(12) states that the application must allow downloading of prescription data into a form that is readable and sortable.

Section 1311.205(b)(13) states that the application must maintain an audit trail related to the following: the receipt, annotation, alteration, or deletion of a controlled

substance prescription; and the setting or changing of logical access controls related to controlled substance prescriptions.

Section 1311.205(b)(14) specifies the information that must be maintained in the audit trail: date and time of the action, type of action, identity of the person taking the action, and outcome.

Section 1311.205(b)(15) states that the application must generate a daily report of auditable events (if they have occurred).

Section 1311.205(b)(16) states that the application must protect the audit trail from unauthorized deletion and shall prevent modification of the audit trail.

Section 1311.205(b)(17) states that the application must back up files daily.

Section 1311.205(b)(18) states that the application must retain records for two years from the date of their receipt or creation.

Section 1311.210 sets the requirements for digitally signing the prescription as received and archiving the record. It also sets the requirements for validating a prescription that has the practitioner's digital signature attached.

Section 1311.215 specifies the requirements for auditable events for pharmacy applications. Auditable events must include at least the following: attempted or successful unauthorized access to the application; attempted or successful unauthorized deletion or modification of any records required by part 1311; interference with application operations related to prescriptions; any setting of or changes to logical access controls related to controlled substance prescriptions; attempted or successful interference with audit trail functions; and, for application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or

logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider. The application must run the internal audit once every calendar day and generate a report that identifies any auditable event. This report must be reviewed by the pharmacy. If the auditable event compromised or could have compromised the integrity of the records, this must be reported to DEA and the application service provider, if applicable, within one business day of discovery.

Section 1311.300 specifies the requirements for third-party audits discussed above and includes the option of substituting a certification from an organization and certification program approved by DEA. Audits or certifications must occur before the application may be used to create, sign, transmit, or process electronic controlled substance prescriptions, and whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first. Audits must be conducted by a person qualified to conduct a SysTrust, WebTrust, or SAS 70 audit, or a Certified Information System Auditor who performs compliance audits as a regular ongoing business activity. DEA is seeking comment regarding the use of Certified Information System Auditors.

Application providers must make audit reports available to any practitioner or pharmacy that uses or is considering using the application to handle controlled substance prescriptions. The rule also requires application providers to notify both their users and DEA of adverse audit reports or certification decisions. Users must be notified within five business days; DEA must be notified within one business day.

Section 1311.302 requires application providers to notify practitioners or pharmacies, as applicable, of any problem that they identify that makes the application

noncompliant with part 1311. When providing patches and updates to the application to address these problems, the application provider must inform the users that the application may not be used to issue or process electronic controlled substance prescriptions until the patches or updates have been installed. DEA is requiring that practitioners and pharmacies be notified as quickly as possible, but no later than five business days after the problem is identified.

Section 1311.305 specifies recordkeeping requirements for records required by part 1311.

VI. Incorporation by Reference

The following standards are incorporated by reference:

- FIPS Pub 180-3, Secure Hash Standard (SHS), October 2008.
- FIPS Pub 186-3, Digital Signature Standard (DSS), June 2009.
- Draft NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 8, 2008; Burr, W. et al.
- NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007.

These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-8930 and are available at http://csrc.nist.gov/.

VII. Required Analyses

A. Risk Assessment for Electronic Prescriptions for Controlled Substances

The Office of Management and Budget's E-Authentication Guidance for Federal Agencies (M-04-04) requires agencies to ensure that authentication processes provide the appropriate level of assurance.[40] The guidance describes four levels of identity assurance for electronic transactions and provides standards to be used to determine the level of risk associated with a transaction and, therefore, the level of assurance needed. Assurance is the degree of confidence in the vetting process used to establish the identity of an individual to whom a credential was issued, the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued, and the degree of confidence that a message when sent is secure. OMB established four levels of assurance:

Assurance Level 1: Little or no confidence in the asserted identity's validity.

Assurance Level 2: Some confidence in the asserted identity's validity.

Assurance Level 3: High confidence in the asserted identity's validity.

Assurance Level 4: Very high confidence in the asserted identity's validity.

M-04-04 states that to determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks and identify measures to minimize their impact. The document states that the risk from an authentication error is a function of two factors: (a) potential harm or impact and (b) the likelihood of such harm or impact. NIST SP 800-63-1 supplements M-04-04 and defines the steps necessary to reach each assurance level for identity proofing that precedes the issuance of the

[40] Office of Management and Budget. "E-Authentication Guidance for Federal Agencies" M-04-04. December 16, 2003.

credential; the use of credential once issued; and the transmission of any document "signed" with the credential. In plain language, an e-authentication risk assessment considers two issues:

- How important is it to know that the person who is issued a credential is, in fact, the person whose identity is associated with the credential.
- How important is it to be certain that the person who uses the credential, once it is issued, is the person to whom it was issued.

This risk assessment addresses the level of assurance needed to allow the use of electronic prescriptions for controlled substances. This section summarizes the assessment that DEA conducted for the interim final rule. The full risk assessment is available in the docket.

As discussed in Section IV J of this preamble, M-04-04 requires that an Agency assess risks as low, moderate, or high for six factors (see Table 1), then determines the Assurance Level needed based on the ratings. Table 3 presents the ratings DEA developed in its risk assessment for the proposed rule and the rationale for each (for the full discussion, see 73 FR 36731-36739).

Table 3: Initial Rating of Potential Impacts for Authentication Errors for Electronic Prescriptions for Controlled Substances

Potential Impact	Initial Rating	Rationale
Inconvenience, Distress, or Damage to Standing or Reputation	Moderate -- At worst, serious short term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.	Identity theft, issuance of illegitimate prescriptions in a practitioner's name, or alteration of prescriptions could expose practitioners to legal difficulties and force them to prove that they had not used an electronic prescription application or issued specific prescriptions.
Financial Loss	N/A	
Harm to Agency Programs or	High -- A severe or	Were there identity theft or the

Potential Impact	Initial Rating	Rationale
Public Interests	catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of (sic) to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.	misuse of a credential issued to a registrant, the potential exists for widespread and rapid diversion of controlled substances. Such diversion would undermine the effectiveness of prescription laws and regulations of the United States. This diversion would, by its very nature, harm the public health and safety, as any illicit drug use does. Such diversion would undermine the effectiveness of the entire United States closed system of distribution created by the CSA and would, for the same reason, be incompatible with United States obligations under international drug control treaties.
Unauthorized release of Sensitive Information	N/A	
Personal Safety	High – A risk of serious injury or death.	Failure to limit the potential for diversion could result in an increase in drug abuse and in the associated deaths and illnesses as well as other social harms
Civil or Criminal Violations	High – A risk of civil or criminal violations that are of special importance to enforcement programs.	A practitioner whose identity was stolen to gain a credential or whose credential was used by someone else to issue a prescription for a controlled substance could be subject to legal action in which the practitioner would have to prove that he was not responsible for the prescriptions. Such legal action against the practitioner could include criminal prosecution, civil fine proceedings, and administrative proceedings to revoke the practitioner's DEA registration.

Under M-04-04, the overall rating is driven by the highest rating assigned.

Therefore, the potential impact of not being able to limit authentication credentials to

DEA registrants is rated as high, which means that without mitigating factors, DEA should impose requirements that meet Assurance Level 4 under NIST SP 800-63-1.

Mitigating Factors

DEA included a number of elements in the interim final rule that mitigate the risks of unauthorized access to the electronic prescription application and reduce the potential for diversion. While some of these relate to authentication to the application, others relate to use of the application itself.

Separation of duties. DEA's premise for its requirements regarding the access to any electronic prescription application to prescribe controlled substances rests on the principle of separation of duties. The interim final rule requires that practitioners wishing to prescribe controlled substances undergo identity proofing by an independent third-party credential service provider (CSP) or certification authority (CA) that is recognized by a Federal agency as conducting identity proofing at the basic assurance level (Assurance Level 3 for CAs) or greater. The CSP or CA will then issue the credential. This approach removes the electronic prescription application provider from the process of issuing the credential, which limits the ability of individuals at the application provider to steal identities and ensures, to as great an extent as possible, that a person will not be issued a credential using someone else's identity.

Access Control. The possession of a credential by the practitioner, while necessary to legally sign controlled substance prescriptions, is not sufficient to do so. After the practitioner has obtained the credential, a person in the practitioner's office (assuming that the practitioner is in private practice in an office setting) must enter information into the electronic prescription application identifying the practitioner as a

person authorized to prescribe controlled substances. A second person in that office, who must be a DEA registrant, must approve the information entered and grant the practitioner access to the electronic prescription application for the purpose of signing controlled substance prescriptions using the practitioner's credential. (Note that a similar system involving separation of duties is being implemented for institutional practitioners, i.e., hospitals and clinics. That system has similar conceptual requirements, but involves different people in the physical processes.)

This separation of duties ensures that even if someone is able to impersonate a practitioner and obtain a credential from an independent third-party CSP or CA, that impersonator will not be able to gain access to the electronic prescription application to sign controlled substance prescriptions unless the impersonator also has the assistance of two persons (one of whom is a DEA registrant) within a practitioner's office. In this way, it will be significantly more difficult for impersonators to gain access to sign controlled substance prescriptions, reducing the possibility of authentication errors and lessening the potential for diversion.

Use of two-factor authentication. DEA is requiring the use of two-factor authentication. Assurance Level 4 requires a hard token that is separate from the computer to which the person is gaining access, but also imposes more stringent requirements on the cryptographic module and the token. DEA has determined that combining the requirements for Assurance Level 3 tokens (i.e., FIPS 140-2 Security Level 1 tokens used in combination with another factor to reach Assurance Level 3) with the requirement that the token be separate from the computer will provide sufficient security to mitigate the risk of misuse. Keeping the token separate from the computer

being accessed makes it much easier for the practitioner to control access to his credential. A person would have to obtain both the token and the second factor to gain access. (Note that DEA is also permitting the use of biometrics as one of the factors that may be used for authentication; the biometric could replace either the hard token or the knowledge factor.)

Application Requirements. In addition to the requirements discussed above, DEA is also imposing the following requirements on the electronic prescription application that will mitigate the risks:

- The application must have the ability to set logical access controls as discussed above and limit access to indicating that prescriptions are ready for signing and signing prescriptions to DEA registrants or those exempted from registration.
- The application must require the use of the two-factor credential to sign the prescription and digitally sign and archive the record when the two-factor authentication protocol is executed. This step ensures that there is a record of the prescription as signed and allows other people in the practice or facility to add information not required by DEA, (e.g., pharmacy URLs) or review the prescription before transmission.
- The application must not allow a practitioner to sign a prescription if his credential is not linked to the DEA number listed on the prescription.
- The application must undergo a third-party audit to determine whether it complies with the requirements of the interim final rule.

In addition, as part of their approval by the Federal government, CSPs and CAs issuing credentials undergo third-party audits to ensure compliance with Federal government standards.

Conclusion

Consistent with M-04-04, DEA believes that it is appropriate for the agency to accept lower level credentials in view of the mitigating factors discussed above. M-04-04 states, in pertinent part (in Section 2.5):

> Agencies may also decrease reliance on identity credentials through increased risk-mitigation controls. For example, an agency business process rated for Level 3 identity assertion assurance may lower its profile to accept Level 2 credentials by increasing system controls or 'second level authentication' activities.

Following this approach, DEA has concluded that, even though the agency rates overall identity assurance for electronic prescribing of controlled substances at Assurance Level 4, the agency believes that Level 3 credentials are acceptable in view of the system controls that are mandated by this interim final rule. Specifically, DEA believes that the requirements that the interim final rule imposes for identity proofing, logical access controls, the separation of the hard token from the computer being accessed, and the application requirements lower the potential for a nonregistrant to steal an identity or gain access to a registrant's credential and issue illegal prescriptions sufficiently to render acceptable remote identity proofing, consistent with NIST SP 800-63-1 Assurance Level 3 requirements, and the use of FIPS 140-2 Security Level 1 hard tokens that in combination with a second factor provided that the token is not stored on the computer to which the person is gaining access. With these requirements in place, the potential for diversion through misuse of a credential will be limited, which supports the closed

system of control DEA is mandated to maintain, protect practitioners from misuse of their identity, and protects the public from the harm of drug abuse. (Note that DEA is not imposing any requirements on the security of the transmission.)

As has been discussed previously, it is important to note that the electronic prescribing of controlled substances is voluntary — practitioners may still dispense controlled substances through the use of written prescriptions, regardless of whether they choose to write controlled substances prescriptions electronically. Also, the compromise of an authentication protocol through loss, credential invalidation, or other cause, does not invalidate the practitioner's authority to write controlled substances prescriptions. Practitioners may continue to write controlled substances prescriptions on paper or generate a prescription electronically to be printed and signed manually even if their authentication credential has been compromised, so long as the practitioner continues to possess a DEA registration.

B. Executive Order 12866

Under Executive Order 12866 (58 FR 51735, October 4, 1993), DEA must determine whether a regulatory action is "significant" and, therefore, subject to Office of Management and Budget review and the requirements of the Executive Order. The Order defines "significant regulatory action" as one that is likely to result in a rule that may:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal government or communities.

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency.

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs or the rights and obligations of recipients thereof.

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the Executive Order.

A copy of the Economic Impact Analysis of the Electronic Prescriptions for Controlled Substances Rule can be obtained by contacting the Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152, Telephone (202) 307-7297. The initial analysis is also available on DEA's Diversion Control Program Web site at http://www.deadiversion.usdoj.gov.

Comments

DEA conducted an initial economic analysis of the proposed rule and sought comments. DEA received several comments regarding the estimates provided in the NPRM.

Comments. A practitioner organization stated that DEA underestimated the costs for registration, hard token hardware and software, software upgrades, annual system audits, and, especially, for separate prescribing workflows for controlled drugs. The commenter asserted that the analysis did not include the added costs for each prescriber every time a controlled substance prescription is written. The commenter believed that the comparison should not be with the current system where controlled substance prescriptions require a separate workflow, but rather with a commenter-preferred system

where all prescribing takes place in a single workflow. The commenter asserted that the costs of prosecutions are dwarfed by the potential benefits offered by a single, manageable electronic prescribing system. The commenter stated that DEA acknowledged in the analysis it did not have valid data on all costs to society from diversion of controlled substances. Without valid estimates of the cost of the problem, the commenter asserted, it is impossible to justify the expense of the proposed solution.

DEA Response. DEA disagrees with this comment, but notes that the revisions to the interim final rule reduce the costs and the additional keystrokes. The only change to the usual workflow will be the use of the two-factor authentication credential to sign the prescription. Wherever possible, in the economic analysis of the interim final rule, DEA has used estimates based on current prices.

DEA's concern is not simply or primarily with the costs of prosecutions, but with the diversion of controlled substances and the societal harm caused by abuse of these drugs. The cost of emergency room treatment alone for people using prescription controlled substances for non medical reasons is far higher than the cost of this rule. Without appropriate security measures, electronic prescriptions could facilitate increased drug abuse, with a concomitant increase in deaths, medical treatment, and other societal costs associated with drug dependency.

Although DEA supports electronic prescribing and shares the hope that it will reduce adverse drug events and improve the efficiency of the healthcare system, there is little, if any, evidence that electronic prescribing is achieving this goal. The limited studies that have examined the impacts of electronic prescribing have found that the primary benefit is improved formulary compliance. DEA has not found any studies that

quantify the number of adverse drug events associated with illegible prescriptions. The data often cited regarding medication errors are based primarily on inpatient hospital and long-term care facility adverse drug events and include "errors" that are unrelated to legibility (e.g., administering a drug to the wrong patient, dispensing the wrong drug); some of the errors cited may not result in adverse drug events (e.g., failing to include all of the label information or the insert). In addition, as discussed below in the Benefits section, studies of pharmacy experiences with electronic prescriptions have found that there may be an increase in errors with these prescriptions. DEA notes that although illegible handwritten prescriptions are unquestionably a problem, in most cases the pharmacists resolve the problem by calling the practitioner to clarify the prescription rather than risk dispensing the wrong drug.

Comments. A pharmacy organization asserted that unless there is a compelling law enforcement need, DEA must eliminate provisions that increase the burden and costs on prescribers and pharmacies. The commenter claimed that these burdens and costs will fall disproportionately on independent, rural and small primary care and physician practices, pharmacies and health care facilities and programs. State pharmacy associations stated that DEA should perform an economic analysis that details the financial impact on safety-net clinics using appropriate metrics (net revenue) and actual fees, and that DEA should consider options that reduce these identified costs. One organization indicated that the analysis did not adequately address the cost of storage, technology, staff resources, and oversight.

DEA Response. DEA disagrees that the costs fall disproportionately on small or rural practices. Most of the costs of the rule will be borne by practitioners, to obtain

identity proofing, and the application providers. DEA has revised the process for identity proofing to reduce the burden on rural practitioners. The primary cost will be to complete an application for a credential or digital certificate and to pay for the credential. The frequency with which a practitioner must do this will be determined by the credential service provider or certification authority.

Although the application providers will have to recover their costs from their customers, the incremental costs for any single customer will be low, particularly when compared to the cost of an electronic health record application. DEA has revised the rule to reduce the costs to application providers by both lengthening the time between audits/certifications and allowing them to substitute certification by an approved organization, where one exists, for a third-party audit. Because the American Recovery and Reinvestment Act requires that an application be certified before a practitioner will be eligible for an incentive payment, it is reasonable to assume that all electronic prescription application providers will be seeking certification and incurring those costs regardless of DEA's rules. On the pharmacy application side, the third-party audit will only need to address compliance with DEA's requirements, most of which existing pharmacy applications already meet.

DEA has removed the requirement for offsite storage. As for the costs for technology, staff resources, and oversight, these apply to acquisition of the application, not to DEA's requirements. DEA is not requiring any registrant to issue or accept electronic prescriptions for controlled substances. Any registrant that purchases an application will incur these costs whether they use the application for controlled substance prescriptions or not.

Comments. An organization representing dentists stated that the number of dentists used in the calculations in the economic analysis was high; the commenter noted that the Bureau of Labor Statistics lists 161,000 dentists as opposed to DEA's estimate of 170,969. The commenter also asserted that DEA did not include potential practitioner reprogramming cost(s) in this figure. The commenter believed that the addition of any reprogramming costs will make this figure much greater and create additional burden for practicing dentists who wish to transmit prescriptions for controlled substances electronically.

DEA Response. In the interim final Economic Impact Analysis, DEA used the organization's estimate for the number of dentists, adjusted to account for growth. DEA has estimated the cost for reprogramming, but notes that this will be done by the application provider, not at the practice level. Unless an individual practice decides to implement biometrics as part of their two-factor authentication credentials, there should not be additional hardware or software needed; the software needed to use a biometric can be relatively inexpensive. DEA expects that there will be considerable variation in the extent of reprogramming an application provider needs to do based on the degree to which an application already meets the requirements being implemented in this rule. Application providers, however, routinely reprogram their software to add new features, upgrade functions, and fix problems. Reprogramming to meet the interim final rule is likely to occur as part of this routine process.

Comments. A pharmacy organization asserted that the cost of dispensing for the average independent community pharmacy is already high. The commenter believed that the regulation would necessitate the purchase of new technology, generating more reports

at the end of the day, and then storing those corresponding reports for five years. The commenter claimed that these processes will only add to the monetary costs and time constraints that pharmacists have to abide by to responsibly consult with and serve their patients. The commenter asserted that such gains from electronic prescribing are relatively minimal when compared to such costs, considering that independent community pharmacies already connected for electronic prescribing only receive around 2 percent of their prescriptions through such technology.

DEA Response. DEA is not requiring any pharmacy to accept electronic prescriptions for controlled substances. Based on industry comments, the existing pharmacy applications already have most, if not all, of the functions that DEA is requiring. It is unlikely, therefore, that any pharmacy will have to replace its existing application. Where additional functionality is needed, it can be added as an upgrade or patch, as occurs routinely with most widely used software applications. The only reports that will be generated are on security incidents, which should be rare events. Pharmacies should not have daily reports to review. DEA has revised the record retention period to two years. DEA also notes that in allowing electronic prescriptions, it is relieving pharmacies of the burden of storing paper prescriptions.

Comments. A pharmacy organization asserted that costs of several cents per prescription will be significant to some pharmacies.

DEA Response. DEA estimates that the average cost of the rule will be less than one cent per controlled substance prescription, which as some commenters noted is far less than the $0.30 per prescription fee some commenters stated they are paying intermediaries.

Comments. A healthcare system stated that PDAs may not be able to function as tokens and thumb drives would require software changes and take too much time to connect. The commenter believed that other solutions would be more expensive. The commenter also noted that mid-level practitioners would be likely to use the same kind of tokens as practitioners, which differed from the assumptions DEA made in its initial analysis. That commenter and a second healthcare system also stated that the initial Economic Impact Analysis did not include staff time for audits.

DEA Response. DEA has not included PDAs in its cost analysis of the interim final rule although some practitioners may use them. The range of possible tokens is considerable and the costs associated with them wide. For example, one-time-password (OTP) devices are slightly more expensive than smart cards or tap-and-go cards, but do not require a separate reader. Where readers are needed, they may exist on keyboards, or can be separate devices. Because it has no basis for estimating how many computers would need readers, DEA has based its cost estimates on OTP devices, recognizing that practices may find other options more suitable.

DEA has not estimated staff time for application providers for audits in part because the interim final rule limits the audit to determining whether the application meets DEA's requirements. An auditor will usually make this determination by testing the application, which will not involve provider staff time. In addition, DEA assumes that once a certification organization is ready to make this determination as part of its certification process, application providers will not need audits. They will obtain the certification for reasons other than compliance with DEA rules.

Comments. An application provider stated that financial incentives may speed adoption more quickly than assumed in the initial Economic Impact Analysis. It further stated that the average salary of a primary care physician is $104,000, but provided no sourcing for this assertion.

DEA Response. DEA has increased (i.e., shortened) the implementation rate to account for the financial incentives that may be available to practitioners. According to the Bureau of Labor Statistics the average salary rate for a physician in family practice is $167,970 (May of 2008). Some hospital-based physicians have lower salary rates, but their costs are likely to be borne by the institutional practitioner.

Comments. An application provider estimated that cost per unit for two-factor authentication at $329 to $349, comprising a hand-held reader at $300, a desktop reader at $20, and a smart card ($29). The commenter estimated support costs between $300 to $400 a year per prescriber to deal with malfunctions. The commenter asserted that it would take 3 to 7 days to replace the smart card. The commenter further indicated that its current support metrics indicate 7 trouble tickets per year per prescriber, 10 percent of which require an office visit. The commenter claimed that the average prescriber writes six controlled substance prescriptions a week and would not pay as much as DEA indicated the costs would be to write controlled substances prescriptions electronically. It noted that these costs would disproportionately burden stand-alone electronic prescription applications because they represent a higher proportion of the annual fee. The commenter indicated that the first year cost of $629-749 would be a 35 percent increase in the $2000 first year fee. Subsequent year costs ($300-400) would be a 58% increase in the $600 charge. The costs represent a much smaller percentage of EHR costs. The

commenter asserted that these costs would deter practitioners from adopting electronic prescribing.

DEA Response. DEA notes that most of the costs the commenter estimated relate to a hand-held reader, but the commenter failed to explain why this was needed. It also failed to explain why the smart card would cost so much, when many are available for a tenth the amount listed, and why it would take days to replace the card. If the practitioner acquires the card locally, then registers or activates the credential, replacement would take little time. The commenter appears to be incurring the support costs for problems already. It is unclear to DEA, based on the commenter's comments, why the commenter believes this would change or increase. Under the interim final rule, the application provider is not involved in providing the authentication credential. If its application has problems after it has been programmed, that is not a cost that accrues to the interim final rule. DEA recognizes that any incremental costs will represent a higher proportion of the annual fee for stand-alone electronic prescription applications. DEA notes, however, that the Federal incentive payments available under the American Recovery and Reinvestment Act are for EHR applications, not electronic prescription applications. It is likely, therefore, that the trend toward EHRs rather than stand-alone electronic prescription applications will accelerate.

The Interim Final Rule Analysis

DEA has determined that this interim final rule is an economically significant regulatory action; therefore, DEA has conducted an analysis of the options. The following sections summarize the economic analysis conducted in support of this rule. DEA is seeking further comments on the assumptions used in this revised economic

analysis and is especially interested in any data or information that commenters can provide that would reduce the many uncertainties in the estimates as discussed below and improve the options considered in the analysis of a final rule.

Options Considered

DEA considered three options for the electronic prescribing of controlled substances:

Option 1: The interim final rule as described in this preamble.

Option 2: The interim final rule with the requirement that one of the factors used to authenticate to the application must be a biometric.

Option 3: No additional requirements for electronic prescription or pharmacy applications, but a callback for each controlled substance electronic prescription.

Universe of Affected Entities

The entities directly affected by this rule are the following:

- DEA individual practitioner registrants who issue controlled substance prescriptions or individual practitioners who are exempt from registration and who are authorized to issue controlled substance prescriptions under an institutional practitioner's registration.
- Hospitals and clinics where practitioners may issue controlled substance prescriptions.
- Pharmacies

In addition, application providers are indirectly affected because their applications must meet DEA's requirements before a registrant may use them to create or process controlled substance prescriptions. The practitioners who prescribe controlled substances

are primarily physicians, dentists, and mid-level practitioners. Hospitals and clinics will be affected if practitioners working for or affiliated with the hospital or clinic use the institutional practitioner's application to issue prescriptions for persons leaving the institution (inpatient medical orders are not subject to these rules). Several thousand institutional practitioner registrants (e.g., prisons, jails, veterinarians, medical practices, and Federal facilities) are not included either because they are unlikely to have staff issuing prescriptions, are already counted in the practitioner total, or, in the case of Federal facilities, already comply with more stringent standards. Table 4 presents the estimates of entities directly affected and estimated growth rates, which are based on recent trends. As the number of hospitals and retail pharmacies have been declining, DEA did not project growth (or decline) for these sectors.

Table 4: Universe of Directly Affected Entities

	In Offices/ In Hospitals	Growth Rate
Physicians	328,772 169,337	2.1 percent*
Mid-levels	82,579 48,841	2.2 percent
Dentists	171,328 N/A	1.3 percent
Total Practitioner	**582,729** **218,178**	1.9 percent
Hospitals and Clinics	12,412	DEA assumes no future growth.
Pharmacies	65,421	DEA assumes no future growth.

* This rate does not include physicians in hospitals.

The number of application providers is based on the number of providers currently certified by SureScripts/RxHub or CCHIT. For practitioners, that number is about 170, which DEA assumes will increase to 200 by the third year and then begin declining. Pharmacy application providers are estimated to be about 40; the actual

number is lower but DEA increased the number to account for pharmacy chains that may have developed their own applications.

The number of controlled substance prescriptions written is relevant to the estimate of cost-savings. DEA estimates the number of prescriptions based on the assumption that the percentage of controlled substance prescriptions in the top 200 brand name and top 200 generic drug prescriptions is the same as it is for the remainder of the prescriptions.[41] According to data from SDI/Verispan, in 2008, controlled substances represented about 12 percent of prescriptions for the top 400 drugs.[42] IMS Health data reported a total of 3.8431 billion prescriptions in 2008.[43] Based on these data, DEA estimates that, with a three percent growth rate for prescriptions, there will be about 475 million controlled substance prescriptions in Year 1 of the analysis. IMS Health data indicate that about 86 percent of prescriptions are filled at retail outlets, which is relevant to estimating public wait time as long-term care prescriptions and mail order prescriptions will not be affected. Previous DEA analysis has indicated that 75 percent of controlled substance prescriptions are original prescriptions or 356 million prescriptions in Year 1. DEA has previously estimated that about 19 percent of prescriptions are currently faxed or phoned into pharmacies. Applying both the 86 percent and 19 percent to the number of original prescriptions results in an estimate of 247 million prescriptions that may have reduced public wait time as electronic prescriptions for controlled substances is implemented.

Unit Costs

[41] The top 400 drugs represent about 87% of all prescriptions dispensed at retail.
[42] See www.drugtopics.com for the top 200 generic and top 200 brand name drugs.
[43] See www.imshealth.com. IMS Health data are used for total prescriptions because the data include prescriptions for long-term care and mail order.

For the interim final Economic Impact Analysis, DEA based all labor costs on May 2008 BLS data, inflated to 2009 dollars and loaded with fringe and overhead. Using BLS data provides a consistent source of data. For the NPRM, DEA used other estimates for physician and dentist costs, but these were based on salary surveys that may be weighted toward larger practices and were not clearly wage as opposed to compensation figures. The effect of the change is to lower the wage rates for these practitioners.

Practitioners will have to complete an application to apply for identity proofing and a credential. As these applications generally ask for standard information that practitioners will be able to fill in without needing to collect documents that they would not carry with them (e.g., credit cards, driver's licenses), DEA estimates that it will take them 10 minutes to complete the form. Credential providers generally require subscribers to renew the credential periodically. This renewal can take the form of an e-mail request that is signed with the credential. To be conservative, DEA estimates that it will take 5 minutes to renew.

For hospitals and clinics, DEA estimates that practitioners and someone at the credentialing office will spend 2 minutes to verify the identity document presented. Practitioners are assumed to take 30 minutes total for this process because they will need to go to the credentialing office. This review will occur only when the hospital or clinic first implements controlled substance electronic prescribing and will involve only those practitioners that already work at or have privileges at the hospital or clinic. All practitioners that are hired or gain privileges later will have this step done as part of their regular initial credentialing.

Prior to granting access, someone at each office must verify that each practitioner has a valid DEA registration and State authorization to practice and, where applicable, dispense controlled substances. As this requires nothing more than checking the expiration dates of these documents, which are often visibly displayed, DEA estimates that this will take an average of one minute. In small practices, which are the majority of offices, it may take no time because the registrant will be one of the people granting access and the status of every registrant will be known. Checking registrations and State authorizations is done as part of credentialing at hospitals and clinics and is, therefore, not a cost of the rule. Similarly, once the rule is implemented at offices, it should not be a cost because credentials should be checked before a person is hired.

Prior to granting access, those who will be given this responsibility will need to be trained to do so. DEA estimates the time at one hour per person at practices. This estimate may be high, particularly for smaller offices. It may also be the case that in some larger practices, people already perform this task for other reasons and training may be unnecessary. Because it is likely that in larger pharmacies, access controls are already being set, DEA estimates that the training time will be five minutes.

DEA estimates that it will take, on average, five minutes to enter the data to grant access for the first time at a practice or a pharmacy. The approval of the data entry is estimated to take one minute. The actual approval may take only a few seconds, but the approver may take time away from some other work, but would presumably do it when using the computer for other tasks.

DEA has not estimated the cost of setting logical access controls at hospitals because hospital applications should already do this. The CCHIT criteria for in-patient

applications include logical access controls; the HL7 standard used by most hospitals includes logical access controls. In addition, an application used by as many different departments as exist at hospitals necessarily will impose limits on who can carry out certain functions. Consequently, DEA's requirements should not entail any actions not already being performed.

Auditable events reported on security incident logs should be rare once the application has been implemented and staff understand their permission levels. Because of the size of hospitals and clinics and the volume of controlled substance prescriptions at pharmacies, DEA estimates that each of them will review security incident logs monthly; DEA estimates that the review will take hospitals ten minutes per month and pharmacies five minutes per month. Because of the smaller size of private practices and the much lower volume of controlled substance prescriptions issued, DEA estimates that a review will be needed only once a quarter. The review time remains at 5 minutes.

DEA estimates that reprogramming for electronic prescription applications will take, on average, 2,000 hours, an estimate based on industry information obtained during the development of DEA's Controlled Substances Ordering System rule.[44] The requirements for pharmacy applications are simpler and include functionalities that the industry has indicated it already has, so DEA assumes an average of 1,000 hours of reprogramming for pharmacy applications.

To estimate the cost of obtaining identity proofing from a credential service provider, DEA used the fee SAFE BioPharma charges for a three-year digital certificate

[44] "Electronic Orders for Controlled Substances" 70 FR 16901, April 1, 2005; Economic Impact Analysis of the Electronic Orders Rule available at http://www.DEAdiversion.usdoj.gov/fed_regs/rules/2005/index.html

and a hard token using remote identity proofing ($110). This figure may be high because it assumes a medium rather than the basic assurance level that DEA is requiring. Based on standard industry practice for digital certificates, DEA estimates that the credential will need to be renewed every three years, but that a complete reapplication will not be required until the ninth year. These assumptions are based on the standards incorporated in the Federal PKI Policy Authority Common Policy. The cost for the three-year renewal is estimated to be $35.00, which is what SAFE charges for a three-year digital certificate at the basic assurance level. Hospitals and clinics are assumed to use or adapt their existing access cards to store the credential and, therefore, incur no additional costs for the credential.

In the initial years, application providers may have to obtain a third-party audit to determine whether the application meets the requirements of the rule. DEA estimates the cost of this audit at $15,000. This estimated cost is about 50 percent of the application fee for CCHIT testing and certification of a full ambulatory electronic health record application ($29,000). DEA chose to use the CCHIT fees as a basis because the interim final rule narrows the scope of the third-party audit and allows a larger number of auditors to conduct the audit. The higher cost estimates in the NPRM were based on obtaining particular types of audits and having the audits cover functions that will not be subject to auditing for installed applications. In addition, the one commenter that already obtained the third-party audits specified in the NPRM stated that the costs were much lower than DEA had estimated. DEA estimates that within five years, all electronic prescription application providers will obtain certification from an approved certification

organization; because the providers already seek these certifications for other reasons, the cost of continuing to obtain certifications will not accrue to the rule after that point.

Table 5 presents the unit costs for both labor-based costs and fees.

Table 5: Unit Costs

Requirement	Item, or labor, required.	Unit Cost
Non-Labor Costs		
Identity proofing and credential	Remote identity proofing and downloadable code for registrant (includes hard token).	$110.00
Renewal of credential	Three-year renewal	$35.00
	Nine-year renewal	$110.00
Initial audit of application	Certification that application meets DEA requirements.	$15,000.00
Reaudit of application	Certification that application still meets DEA requirements.	$15,000.00
Labor Costs		
Application for identity proofing and credential	Registrant must fill out form; 10 minutes required.	$28.23
Renewal application for credential	Registrant must only fill out parts where information has changed; 5 minutes needed.	$14.12
Registration check	Requires one minute for a non-registrant.	
	Physician office—nurse	$1.12
	Dental office—dental assistant	$0.57
Access control —training (practice office)	One hour per person; one is a registrant	
	Physician plus nurse	$259.35
	Mid-level plus nurse	$151.49
	Dentist plus dental assistant	$201.01
Access control—granting (practice office)	Requires one minute for registrant, five minutes for non-registrant (nurse)	
	Physician plus nurse	$8.66
	Mid-level plus nurse	$7.00
	Dentist plus dental assistant	$5.64
Access control—training (pharmacy)	Requires five minutes for pharmacy technician	$2.33
Access control—granting (pharmacy)	Requires five minutes for pharmacy technician	$2.33
Review of security logs (practice office)	Requires five minutes per quarter; 20 minutes per year for nurse.	$22.39
Review of security logs (pharmacy)	Requires five minutes per quarter; 20 minutes per year for pharmacy tech.	$11.43
Review of security logs (hospital)	Requires ten minutes per month per year for system administrator.	$136.64
ID check, face to face (hospital only)	Requires two minutes for HR person AND 30 minutes per hospital practitioner OR 30 minutes per private physician.	$1.20 $55.22 $96.08
Reprogramming applications for practices	Requires 2,000 hours of application provider engineer's time.	$184,197
Reprogramming pharmacy	Requires 1,000 hours of application provider	$92,099

Requirement	Item, or labor, required.	Unit Cost
applications	engineer's time.	

Total Costs

To proceed from unit costs to total costs, it is necessary to establish the frequency of occurrence of cost items and the distribution of those occurrences, and thus of costs, over time. DEA assumes that all application providers will reprogram their applications in the first year and that after the fifth year they will be able to substitute certification for the third-party audit. DEA assumes that pharmacies will be able to accept electronic prescriptions in the first year and set initial access controls in that year, but that they will incur ongoing costs for checking security incident logs. Hospitals and clinics are assumed to adopt applications within five years; identity proofing costs occur only in the first year of adoption. Practitioners are assumed to adopt electronic prescribing over seven years; after that point implementation for practitioners basically covers new practitioners and offices as well as ongoing costs. Practitioners incur ongoing costs for renewal of the credential, reviewing security incident logs, and adding new staff to the access list. DEA estimates costs for 15 years. Table 6 presents the implementation rate for practitioners.

Table 6: Implementation Rates for Practitioners

	Implementation Rate (percentage)	Cumulative Percentage
YEAR 1	6.0	6.0
YEAR 2	10.0	16.0
YEAR 3	20.0	36.0
YEAR 4	20.0	56.0
YEAR 5	20.0	76.0
YEAR 6	10.0	86.0
YEAR 7	5.0	91.0
YEAR 8	2.0	93.0
YEAR 9	1.0	94.0

	Implementation Rate (percentage)	Cumulative Percentage
YEAR 10	1.0	95.0
YEAR 11	1.0	96.0
YEAR 12	1.0	97.0
YEAR 13	1.0	98.0
YEAR 14	1.0	99.0
YEAR 15	1.0	100.0

Total costs are calculated by multiplying the unit cost for an item or activity by the number of entities that will incur the cost in each year. Tables 7 and 8 present the Option 1 annualized costs by item and regulated entity at both a 7 percent and 3 percent discount rate.

Table 7: Option 1 Annualized Costs by Item and by Sector--7.0 percent

	Practitioners' Offices	Hospitals	Pharmacies	Application Providers	Totals
Credential	$14,669,488				$14,669,488
Credential application	$3,844,882				$3,844,882
Registration check	$30,405				$30,405
Granting access	$303,086		$16,752		$319,838
Training for granting	$7,147,886		$50,255		$7,198,142
Review security logs	$4,248,868	$1,524,079	$1,959,040		$7,731,986
ID verification		$4,717,580			$4,717,580
Reprogram applications				$3,842,530	$3,842,530
Obtain certification				$391,021	$391,021
Audit of applications				$583,957	$583,957
Totals	**$30,244,615**	**$6,241,658**	**$2,026,046**	**$4,817,509**	**$43,329,829**

Table 8: Option 1 Annualized Costs by Item and by Sector--3.0 percent

	Practitioners' Offices	Hospitals	Pharmacies	Application Providers	Totals
Credential	$14,761,504				$14,761,504
Credential application	$3,817,785				$3,817,785
Registration check	$27,259				$27,259
Granting access	$281,572		$12,781		$294,353
Training for granting	$6,315,405		$38,342		$6,353,747
Review security logs	$4,399,243	$1,518,215	$1,885,804		$7,803,262
ID verification		$3,834,522			$3,834,522
Reprogram applications				$3,842,530	$3,842,530
Obtain certification				$393,356	$393,356

	Practitioners' Offices	Hospitals	Pharmacies	Application Providers	Totals
Audit of applications				$650,592	$650,592
Totals	**$29,602,769**	**$5,352,737**	**$1,936,927**	**$4,886,478**	**$41,778,910**

Option 2

Option 2 is the same as Option 1, except that the two-factor authentication credential requires a biometric identifier and a hard token. Passwords would not be permitted as an authentication factor. The cost items are:

- Biometric readers for practitioners' offices, hospitals, and clinics
- Software packages for practitioners' offices and clinics
- Reprogramming of applications for hospitals

A biometric reader would be needed for every practitioner's computer. DEA estimates that hospitals would need one for every 15 beds, and each clinic would need an average of two readers. Based on American Hospital Association data, DEA estimates the number of community hospital beds to be 802,658. The number of clinics is estimated to be 7,485. There are 20 firms providing applications to hospitals, and their number is not expected to change.[45] All of these firms would reprogram their applications in YEAR 1. Costs of readers and software packages would be incurred as hospitals and clinics adopt electronic prescriptions for controlled substances. Hospital beds and clinics are phased in as shown in Table 9.

Table 9: Phase-in of Hospital Beds and Clinics

	Beds	Clinics
YEAR 1	200,665	1,871
YEAR 2	200,665	1,871

[45] The estimate is based on the number of application providers that have obtained CCHIT certification for inpatient EHRs.

	Beds	Clinics
YEAR 3	160,532	1,497
YEAR 4	160,532	1,497
YEAR 5	80,266	749

There are no costs for hospitals and clinics after YEAR 5. All reprogramming costs are in YEAR 1. Costs for practitioners' offices and registrants extend over 15 years following the projected start-up of electronic prescriptions for controlled substances in practitioners' offices and number of registrants in practitioners' offices starting electronic prescriptions for controlled substances.

A biometric reader that meets the requirements costs $114.00.[46] The software package for clinics and offices is $86.00. Reprogramming of applications for hospitals would require 200 hours for an application provider's engineer at $92.10 per hour. Cost is $18,420 per application provider. Table 10 presents the annualized costs of adding the biometric.

Table 10: Cost of Option 2

	7.0 percent	3.0 percent
YEAR 1	$8,037,011	$8,037,011
YEAR 2	$10,862,145	$11,283,976
YEAR 3	$18,424,735	$19,883,569
YEAR 4	$17,750,891	$19,900,309
YEAR 5	$16,454,640	$19,163,490
YEAR 6	$8,085,656	$9,782,458
YEAR 7	$4,387,114	$5,513,892
YEAR 8	$2,278,677	$2,975,149
YEAR 9	$1,570,416	$2,130,037
YEAR 10	$1,502,772	$2,117,445
YEAR 11	$1,437,996	$2,104,861
YEAR 12	$1,375,970	$2,092,286
YEAR 13	$1,316,578	$2,079,722
YEAR 14	$1,259,712	$2,067,171
YEAR 15	$1,205,265	$2,054,634
Total	**$95,949,579**	**$111,186,009**

[46] Based on the cost of BioTouch 500, which is a separate reader. Where the reader is part of a keyboard, the bundled reader and software is available for $200. The software cost was derived from this price.

	7.0 percent	3.0 percent
Annualized	$10,534,748	$9,313,672
Annualized plus Option 1	$53,864,576	$51,092,582

The cost of the biometrics requirement is additive to the interim final rule cost, since no other requirements are eliminated.

Option 3

Under this option the security requirements of the interim final rule are set aside and sole reliance for security is placed on a requirement that, on receipt of an electronic prescription for a controlled substance, a pharmacy must call the practitioner's office for verification of the prescription. For the sake of simplicity, DEA has not included in this option estimates of the time that will be required to reprogram existing applications to conform to the basic information included on every controlled substance prescription. DEA has no basis for determining how many existing applications do not include or do not transmit all of this information. Similarly, there may be some pharmacy applications that will require reprogramming to incorporate the requirements for annotations. The costs of reprogramming, however, will be relatively small compared with the primary cost of this option.

The cost of this option depends on the number of prescriptions to be verified. There were 461,172,000 controlled substance prescriptions in 2008.[47] Annual growth rate has been 3.0 percent. Therefore, DEA expects 475,007,160 prescriptions in YEAR 1 and growth thereafter at 3.0 percent annually. Of these prescriptions, 75.0 percent will be original prescriptions, requiring verification if electronic; the remainder are refills that are

[47] In 2008, controlled substances represented 12.15% of the top 400 brand name and generic drugs sold at retail. The estimated number of controlled substance prescriptions is based on the assumption that 12% of all prescriptions (3.8431 billion according to IMS Health data) are for controlled substances.

authorized on the original prescription and require no contact between the pharmacy and practitioner.

Industry estimates indicate that 30 percent of original prescriptions generate callbacks to deal with formulary issues, requests to change to generic forms of the prescribed drug, illegibility, and other problems. Based on data from a 2004 Medical Group Management Association survey, 34 percent of callbacks on original prescriptions were for formulary issues, 31 percent were about generic drugs, and 35 percent were on other issues.[48] The callback rate for controlled substance prescriptions is likely to be lower than 30 percent because more than 85 percent of controlled substance prescriptions are for generic drugs. Adjusting for a lower number of calls related to generic drugs, DEA estimates that currently 22 percent of controlled substance prescriptions require callbacks. The callback option applies only to new calls that would need to be placed, or 78 percent of the original prescriptions: 277,879,189 (0.78 x 0.75 x 475,007,160). For the 22 percent of prescriptions that already require callbacks, the confirmation would simply be part of a call that is being made anyway and, therefore, is not an additional cost. The number of electronic prescriptions each year requiring calls will be determined by the rate of adoption of electronic prescriptions for controlled substances. Because these are callbacks simply to confirm the legitimacy of the prescription, DEA assumes that each call would require three minutes of a pharmacy technician's time, three minutes of a medical assistant's time, and one minute of the practitioner's time. Table 11 presents the present value and annualized costs of Option 3.

Table 11: Present Value and Annualized Cost Option 3

[48] http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=19248, accessed 08/06/09.

	7.0 percent	3.0 percent
YEAR 1	$100,904,733	$100,904,733
YEAR 2	$259,020,250	$269,079,289
YEAR 3	$561,008,812	$605,428,399
YEAR 4	$840,056,809	$941,777,510
YEAR 5	$1,097,457,393	$1,278,126,621
YEAR 6	$1,195,435,021	$1,446,301,176
YEAR 7	$1,217,649,690	$1,530,388,454
YEAR 8	$1,197,891,176	$1,564,023,365
YEAR 9	$1,165,509,232	$1,580,840,821
YEAR 10	$1,133,874,313	$1,597,658,276
YEAR 11	$1,102,975,819	$1,614,475,732
YEAR 12	$1,072,802,902	$1,631,293,187
YEAR 13	$1,043,344,493	$1,648,110,643
YEAR 14	$1,014,589,338	$1,664,928,098
YEAR 15	$986,526,025	$1,681,745,554
Total	**$13,989,046,006**	**$19,155,081,859**
Annualized	**$1,535,922,056**	**$1,604,555,706**

Table 12: Total Annualized Costs of Options

	7.0 percent	3.0 percent
Option 1	$43,329,829	$41,778,910
Option 2 – Required Use of Biometrics	$53,864,576	$51,092,582
Option 3 – Callbacks	$1,535,922,056	$1,604,555,706

Benefits

Electronic prescriptions are widely expected to reduce errors in medication dispensing because they will eliminate illegible written prescriptions and misunderstood oral prescriptions. They are also expected to reduce the number of callbacks from pharmacy to practitioner to address legibility, formulary, and contraindication issues. Electronic prescriptions may also reduce processing time at the pharmacy and wait time for patients. These benefits are likely to be mitigated to some extent. As a Rand study suggested, practitioners may fail to review the prescription and notice errors that occur when the wrong item is selected from one or more drop-down menus; pharmacists may

be less likely to question a legible electronic prescription.[49] The formulary and contraindication checks are functions that practitioners sometimes disable because they do not work as they should or take too much time.[50] In addition, recent studies indicate that electronic prescriptions sometimes are missing information, particularly directions for use and dosing errors.[51] [52] Nonetheless, electronic prescriptions may provide benefits in avoided medication errors, reduced processing time, and reduced callbacks. These benefits of electronic prescriptions are not directly attributable to this rule because they accrue to electronic prescribing, not the incremental changes being required in this rule.

DEA has quantified three types of benefits: reduced number of callbacks to clarify prescriptions, the reduction in wait time for patients picking up prescriptions, and the cost-savings pharmacies will realize from eliminating storage of paper records. One of the greatest burdens in the paper system is the need for callbacks to clarify prescriptions. Clarifications and changes may be required for several reasons: the prescription is not legible; required information is not included on the prescription; the prescribed dosage unit does not exist; the particular medication is not approved by the patient's health insurance; and the drug prescribed is contraindicated because it reacts with other medications the patient is taking or because it negatively affects other conditions from which the patient suffers. Each callback involves the pharmacy staff and one or more staff at the practitioner's office, often including the practitioner. Electronic

---

[49] Bell, D.S. et al., "Recommendations for Comparing Electronic Prescribing Systems: Results of An Expert Consensus Process," Health Affairs, May 25, 2004, W4-305-317.
[50] Grossman, J.M. et al., "Physicians' Experiences Using Commercial E-Prescribing Systems," Health Affairs, 26, no. 3 (2007), w393-w404.
[51] Warholak, T.L. and M.T. Rupp. "Analysis of community chain pharmacists' interventions on electronic prescriptions." Journal of American Pharm Association, 2009, Jan-Feb; 49(1): 59-64.
[52] Astrand, B. et al., "Assessment of ePrescription Quality: an observational study at three mail order pharmacies." BMC Med Inform Decis Mak, 2009 Jan 26; 9:8.

prescriptions will eliminate illegible prescriptions and could eliminate those with missing information or unavailable dosage units or forms. The recent studies cited above indicate that at least some prescription applications do not prevent practitioners from transmitting electronic prescriptions that are incomplete. At present, the field for directions for use in the NCPDP SCRIPT has not been standardized; when it is, the issues cited in the studies related to these directions may be resolved. Whether formulary and contraindication callbacks are eliminated will depend on the functions of the electronic prescription applications and the accuracy of the drug databases that they use.

The public is also affected by the current system. For the majority of controlled substance prescriptions, the patient (or someone acting for the patient) presents a paper prescription to the pharmacy and then waits for the pharmacy to fill it. The time between the point when the prescription is handed to the pharmacist and the point when it is ready for pick-up is a cost to the public.

The percentage of callbacks that will be eliminated by electronic prescribing is unclear. The Centers for Medicare and Medicaid Services, in its November 16, 2007, proposed rule on formulary and generic transactions, estimated a 25 percent reduction in time spent on callbacks.[53] DEA similarly assumes that callbacks will be reduced by 25 percent. For these callbacks, which require more effort than the simple confirmation required for Option 3, DEA used the time estimates from the MGMA survey (6.9 minutes of staff time per call and 4.2 minutes of practitioner time).[54] Assuming that electronic controlled substance prescriptions phase in over 15 years, as described above, the

[53] 72 FR 64900, November 16, 2007.
[54] http://www.mgma.com/WorkArea/DownloadAsset.aspx?id=19248, accessed 08/06/09.

annualized time-saving for eliminating 25 percent of these callbacks would be $420 million (at 7% discount) or $439 million (at 3% discount).

Electronic prescriptions could also reduce the patient's wait time at the pharmacy. The number of original controlled substance prescriptions that could require public wait time is based on the estimated number of original prescriptions (approximately 356 million in 2009), reduced by 19 percent, to account for those prescriptions phoned to the pharmacy[55] plus another 14 percent to remove those that are currently filled by mail order pharmacies or long-term care facilities.[56] Assuming the average wait time is 15 minutes for the 81 percent of original prescriptions that are presented on paper to retail pharmacies (not mail order or long-term care prescriptions), if those waiting times are eliminated, at the current United States average hourly wage ($20.49), the annualized savings over 15 years would be $1 billion (at 7% discount) or $1.03 billion (at 3% discount).

The estimate for public wait time is an upper bound, as such it is not included in the primary estimate for the benefits of this interim final rule. It assumes that the practitioner will transmit the prescription and that the pharmacist will open the record and fill it before the patient arrives at the pharmacy. Recent research on electronic prescriptions found that 28 percent of electronic prescriptions transmitted were never picked up by patients; for painkillers, more than 50 percent were not picked up.[57] If pharmacies prepared electronic prescriptions before the patient arrives, the pharmacy will

[55] A 1999 Drugtopics.com survey indicated that 36% of all prescriptions were phoned in; because refills are usually authorized on the original prescription and do not require second calls, and slightly less than half of prescriptions are refills, the analysis uses 19% for phoned in prescriptions.
[56] Based on IMS Health 2008 channel distribution by U.S. dispensed prescriptions. http://imshealth.com, accessed June 16, 2009.
[57] Solomon, M., and S.R. Majumdar. "Primary Non-Adherence of Medications: Lifting the Veil on Prescription-filling Behavior" Journal of General Internal Medicine, March 2, 2010.

have spent time for which it will not be reimbursed if the patient does not pick up the prescription and will spend further time returning the drugs to stock and correcting records. It is possible, therefore, that pharmacies will not be willing to fill electronic prescriptions for controlled substances until they are certain that the patient wants to fill the prescription. The primary estimate for public wait time, therefore, is zero.

Table 13 presents the annualized gross benefits at a 7.0 percent and 3.0 percent discount rate.

Table 13: Annualized Gross Benefits

	7%	3%
Callbacks Avoided	$419,745,516	$438,502,110

These benefits are gross rather than net benefits, but it is not possible to compare these cost-savings to the costs of the rule or to estimate net benefits. These savings will accrue to any electronic prescription application. The only way to assess net benefits is to compare them with the costs of the full application and its implementation, not the incremental costs of DEA's requirements.

Pharmacies are required to retain all original controlled substance prescriptions, including oral prescriptions that the pharmacist reduces to writing, on paper for two years. As electronic prescriptions replace paper records, pharmacies will be able to eliminate file cabinets, freeing up space for other uses. The annualized cost of a prescription file cabinet is $78.50 ($715 annualized over 15 years at 7%); the cost of the floor space is $55.34 per cabinet (2.77 square feet times $20/square feet rental price for retail space). The annualized cost-savings for pharmacies are $1.38 million at 7 percent and $1.4 million at 3 percent.

Other Benefits

DEA has not attempted to quantify or monetize the benefits of the rule that relate to diversion because of a lack of data on the extent of diversion of controlled substances through forged or altered prescriptions and alteration of pharmacy records. Electronic prescriptions for controlled substances will directly affect the following types of diversion:

- Stealing prescription pads or printing them, and writing non-legitimate prescriptions.
- Altering a legitimate prescription to obtain a higher dose or more dosage units (e.g., changing a "10" to a "40").
- Phoning in non-legitimate prescriptions late in the day when it is difficult for a pharmacy to complete a confirmation call to the practitioner's office.
- Altering a prescription record at the pharmacy to hide diversion from pharmacy stock.

These are examples of prescription forgery that contribute significantly to the overall problem of drug diversion. DEA expects this rule to reduce significantly these types of forgeries because only practitioners with secure prescription-writing applications will be able to issue electronic prescriptions for controlled substances and because any alteration of the prescription at the pharmacy will be discernible from the audit log and a comparison of the digitally signed records. DEA expects that over time, as electronic prescribing becomes the norm, practitioners issuing paper prescriptions for controlled substances may find that their prescriptions are examined more closely.

The Substance Abuse and Mental Health Services Administration (SAMHSA) runs the Drug Abuse Warning Network (DAWN), a public health surveillance system that monitors drug-related visits to hospital emergency departments and drug-related deaths investigated by medical examiners and coroners. SAMHSA reported that in 2003, in six States (Maine, Maryland, New Hampshire, New Mexico, Utah, and Vermont) there were 352 deaths from misuse of oxycodone and hydrocodone, both prescription controlled substances. SAMHSA data for 2006 show that 195,000 emergency department visits involved nonmedical use of benzodiazepines (Schedule IV) and 248,000 involved nonmedical use of opioids (Schedule II and III). Of all visits involving nonmedical use of pharmaceuticals, about 224,000 resulted in admission to the hospital; about 65,000 of those individuals were admitted to critical care units; 1,574 of the visits ended with the death of the patient. More than half of the visits involved patients 35 and older. Using a value per life of $5.8 million, the costs of the 2003 deaths from misuse of prescription controlled substances in the six States is more than $2 billion.[58] The cost of the 2006 emergency room visits is above $350 million (at $1,000 per visit), not including the cost of further in-patient care for those admitted. These costs are some fraction of the total cost to the nation. DEA has no basis for estimating what percentage of these costs could be addressed by the rule. If, however, the rule prevents even a small fraction of the deaths and emergency care the benefits will far exceed the costs.

These costs also do not represent all of the costs of drug abuse to society. Drug abuse is associated with crime and lost productivity. Crime imposes costs on the victims

[58] The DAWN mortality data from 2005 indicate that almost 4,900 people died with prescription opioids in their bloodstream; about 600 were not using any other drug or alcohol. These numbers, however, do not indicate how many of the people were using the drugs for nonmedical purposes.

as well as on government. DEA does not track information on controlled substance prescription drug diversion because enforcement is generally handled by State and local authorities. The cost of enforcement is, however, considerable. In 2007, DEA spent between $2,700 for a small case and $147,000 for a large diversion case just for the primary investigators; adjudication costs and support staff are additional. It is reasonable to assume that State and local law enforcement agencies are spending similar sums per case. Some cases involve multiple jurisdictions, all of which bear costs for collecting data and deposing witnesses. The rule could reduce the number of cases and, therefore, reduce the costs to governments at all levels. A reduction in forgeries will also benefit practitioners who will be less likely to be at risk of being accused of diverting controlled substances and of then having to prove that they were not responsible.

Adverse drug events that result from medication errors are frequently cited as a benefit of electronic prescriptions. Illegible prescriptions and misunderstood oral prescriptions can result in the dispensing of the wrong drug, which may cause medical problems and, at the very least, fail to provide the treatment a practitioner has determined is necessary. Once a practitioner has access to a patient's complete medication list, electronic prescription applications hold the promise of identifying contraindication problems so that a patient is not prescribed drugs that taken together cause health problems or cancel the benefits. Allergy alerts will also warn practitioners of potential medication concerns.

DEA has not attempted to estimate the extent of these benefits for two reasons. First, there are few data that indicate the extent of the problem as it relates to prescriptions. The data most frequently cited on medication errors and adverse drug

events (1.5 million preventable adverse drug events) are from two literature reviews conducted by the Institute of Medicine.[59] These reviews and the estimate are based on studies that looked at medication errors that occur in hospitals, nursing homes, clinics, and ambulatory settings. Similarly, a 2008 review of studies found fewer errors with electronic medication orders, but at least 24 of the 27 studies reviewed covered only inpatient medication orders, which DEA does not regulate.[60] [61] Many of the studies cover errors that will not be addressed by electronic prescribing, such as inpatient administration errors (i.e., either the chart was incorrect or the chart was correct, but the wrong drug or dosage was administered or the drug was given to the wrong patient), pharmacy dispensing errors (i.e., the prescription was correct, but the wrong drug was given to the patient), failure to include the dosage or other information on the label, and failure to include informational inserts with the dispensed drug. All of these may cause adverse drug events, but will not be addressed by electronic prescribing. Other errors, such as the practitioner's selection of the wrong dose, wrong drug, or wrong frequency of use, may or may not be addressed by electronic prescribing. DEA has no basis to determine what number of adverse drug events could be prevented by the use of an electronic prescription application. Although illegible prescriptions have caused adverse drug events when the wrong drug or dosage was dispensed, most often pharmacies contact the practitioner to decipher prescriptions rather than guess at the drug or dosage intended. In addition, the assumption that the use of electronic prescription applications

[59] "To Err is Human: Building a Safer Health System," IOM 2000; "Preventing Medication Errors," IOM 2007. www.nap.edu.
[60] Ammenwerth, E. et al. "The Effect of Electronic Prescribing on Medication Errors and Adverse Drug Events: A Systematic Review." Jour. Am. Medical Informatics Assn., June 25, 2008.
[61] Most of the studies label all medical orders as prescriptions, whether they are included on a patient's chart in a hospital or LTCF or are written and given to a patient to fill at a pharmacy.

will alert practitioners to contraindications and allergies is based on the assumption that the patient's medical record will be complete. Although this may be the case when every patient has an EHR and all of the applications are interoperable so that a practitioner can access pharmacy records, until that time the medical record will be only as complete as the patient is willing or able to make it, which will limit the ability of the application to alert the practitioner to potential problems. Similarly, until EHRs have databases that link drug names to diagnostic codes and dosage units to age and weight, the applications will have no way to prevent a practitioner from issuing a prescription with an inappropriate drug name or dosage.

Second, the use of electronic prescription applications and transmission systems may introduce errors. Keystroke and data entry errors may replace some of the errors that occur with illegible handwriting. A comment on the proposed rule from a State pharmacy board indicated that, at least at this early stage of implementation, the translation of the electronic data file to the pharmacies has caused data to be placed in the wrong fields and, in some cases, in the wrong patient's file. Similarly, a 2006 survey of chain pharmacy experience with electronic prescribing noted both positive experiences (improved clarity and speed) and negative, prescribing errors, particularly those with wrong drugs or directions.[62]

DEA believes that electronic prescribing will reduce the number of prescription errors, but it has no basis for estimating the scope of the problem or the extent of reduction that will occur and the speed at which it will occur. Some of the problems will not be solved until EHRs are common and linked; others could be addressed more easily

[62] Rupp, M.T. and T.L. Warholack. "Evaluation of e-prescribing in chain community pharmacy: best-practice recommendations." J. Am. Pharm. Assoc. 2008 May-Jun; 48(3):364-370.

by programming applications to require all of the fields to be completed before transmission. Even the best system is unlikely to be able to eliminate human errors.

Uncertainties

Any economic analysis involves some level of uncertainty about elements of the analysis. This is particularly true for this analysis, which must estimate costs for implementation of a new technology and project voluntary adoption rates. This section discusses the elements that have the greatest level of uncertainty associated with them.

The American Recovery and Reinvestment Act (Pub. L. 111-5) provides incentives for practitioners to adopt electronic health record applications; the incentives are scheduled to end after 2016. The analysis assumes that practitioners will adopt electronic prescribing by that time; after that point all of the implementation occurs with new entrants. Whether adoption is, in fact, that rapid will depend on a number of factors unrelated to this rulemaking. The barriers to adoption continue to be the high cost of the applications, which may be greater than the subsidies; the disruption that implementation creates in a practice; and uncertainty about the applications themselves.[63] The pattern with software applications is that a large number of firms enter a market, but the vast majority of them fail, leaving a very few dominant providers.[64] The health IT market is still in the early phases of this process. DEA has no basis for estimating when dominant players will emerge. The 7-year implementation period projected may be too conservative or too optimistic.

---

[63] California HealthCare Foundation, Snapshot: The State of Health Information Technology in California, 2008.

[64] Bergin, T.J., "The Proliferation and Consolidation of Word Processing Software: 1985-1995." IEEE Annals of the History of Computing. Volume 28, Issue 4, Oct.-Dec. 2006 Page(s):48 – 63.

The time for reprogramming existing applications is estimated to be between 1,000 hours and 2,000 hours. DEA based the upper estimate on information provided by the industry for DEA's rulemaking regarding electronic orders for controlled substances. The actual cost to existing application providers is likely to vary widely. Some providers may meet all or virtually all of the requirements and need little reprogramming. Many of the requirements are standard practice for software (e.g., logical access controls for hospitals) and should need minimal adjustments. Most electronic prescription applications appear to present the data DEA will require on prescriptions. Any software firm that uses the Internet for any transaction will have digital signature capability. Electronic health record applications must control access to gain Certification Commission for Healthcare Information Technology certification. Nonetheless, DEA expects that for some existing providers, the requirements may take more than the estimated time. The extent to which this requires additional time will also depend on whether the changes are incorporated into other updates to the application or are done on a different schedule.

Another uncertainty of application provider costs relates to the third-party audit and the time that will elapse before a certification organization is able to certify compliance with DEA's requirements. If the Certification Commission for Healthcare Information Technology includes DEA's requirements in its criteria, the costs for third-party audits may be eliminated sooner than estimated. The interim final rule provides more options for obtaining a third-party audit, which should reduce its cost. DEA has not assumed that any organization will certify pharmacy applications because no organization

currently does so except for determining whether the pharmacy application can read a SCRIPT format.

The single largest cost for practitioners is obtaining identity proofing and an authentication credential. DEA used the cost of a three-year digital certificate at a medium assurance level from the SAFE BioPharma Certification Authority for the cost estimate. SAFE meets the criteria set in the rule. Other firms that meet the criteria provide digital certificates and other credentials for more and for less. The actual cost will not be known until the rule is implemented and practitioners and providers decide on the type of credential they will use. Some commenters on the proposed rule stated that remote identity proofing, which is allowable, can be done very quickly, which could lower the cost. The firms providing the service, however, may impose other requirements beyond those of DEA, which could increase the cost.

There will also be costs associated with lost or compromised credentials. DEA has not attempted to estimate those costs because the frequency with which this will occur and the requirements that credential providers will impose is not known. Some practitioners will never incur these costs while others may incur them multiple times. Credential providers may require a practitioner to go through identity proofing or may impose lesser requirements. If one of the two factors is a password, credential providers may deal with password resets as they do now; password resets do not usually involve issuing a new token or a fee.

C. Regulatory Flexibility Act

Under the Regulatory Flexibility Act of 1980 (5 U.S.C. 601-612) (RFA), Federal agencies must evaluate the impact of rules on small entities and consider less burdensome

alternatives. In its Economic Impact Analysis, DEA has evaluated the cost of the rule on individual practitioners and small pharmacies. The initial costs to the smallest practitioner office will be about $400 ($110 for identity proofing including the authentication credential, and $290 in labor costs to complete the application, receive access control training, and set logical access controls). The main ongoing costs for the rule will be the renewal of the credential ($49 every three years) and checking security logs ($22 per year) plus any incremental cost of the software or application. The initial costs for the basic rule elements represent about 0.3 percent of the annual income of the lowest paid practitioner and 0.1 percent of average revenues. The ongoing costs are considerably lower. For practices with a physician and a mid-level practitioner, the costs would be lower because access control training would not need to involve the physician. (Mid-level practitioners, because they are generally employees, are not small entities under the Regulatory Flexibility Act.)

Determining the incremental cost of the application requirements per practitioner is difficult because it depends on the number of application providers, the number of customers, the number of application requirements that an application provider does not already meet, and how costs are recovered (in the year in which the money is spent or over time). For example, an electronic health record application that had to reprogram to the full extent will have incremental application costs of $199,000 ($15,000 for the third-party audit and $184,000 for reprogramming). If the provider recovered the costs from 1,000 practitioners (charges are usually on a per practitioner, not per practice basis), the incremental cost to those customers will be $199 or about $17 a month. The costs for the application provider in the out years will be much lower ($15,000 every two years)

because no further programming is needed. Even if the application provider did not add practitioners and continued to obtain a third-party audit rather than rely on certification, the incremental cost to practitioners will be less than a dollar a month.

For pharmacies, the costs will be the incremental cost that their application provider charges to cover the costs of reprogramming and audits ($92,000 plus $15,000) plus the cost of reviewing the security log ($11.43 per year) and initial access control training and initial access control setting ($4.66). In the first year, if the application providers recover the programming costs and initial audit costs in a single year, the average incremental cost to a pharmacy for these two activities will be $65 ($4,284,900 first year cost divided by 65,421 pharmacies). The total first year cost will, therefore, be less than $100. After that, the incremental charge to recover the cost of the third-party audit will be $9 per pharmacy every two years, assuming the cost is evenly distributed across all pharmacies. The pharmacy will have continuing labor costs for reviewing security logs ($11.43). The first year charge represents less than 0.01 percent of an independent pharmacy's annual sales. The annual cost is less than $0.01 per controlled substance prescription. It also represents a far lower cost than the pharmacy will pay its application provider to cover the fee charged by SureScripts/RxHub or another intermediary for processing the prescriptions. According to comments DEA received to its notice of proposed rulemaking, the application provider charges a transaction fee of $0.30 per electronic prescription to cover intermediary charges for routing and, where necessary converting, prescriptions to ensure that the pharmacy system will be able to capture the data electronically. Based on National Association of Chain Drug Stores data on the average price of prescriptions ($71.69) and the average value of prescription sales,

an independent pharmacy processes about 36,000 prescriptions a year and will have to pay about $10,800 to cover the transaction fee.[65]

The average annualized cost to hospitals and clinics is about $180, which does not represent a significant economic impact. Most of the hospital tasks are part of their routine business practices related to credentialing.

Application providers are not directly regulated by the rule and, therefore, are not covered by the requirements of the RFA. DEA notes, however, that the costs of the rule are not so high that any of these firms will not be able to recover them from their customers. Reprogramming is a routine practice in the software industry; applications are updated with some frequency to add features and fix problems. The additional requirements of the rule can be incorporated during the update cycle. Many of these firms are already spending more than DEA has estimated to obtain CCHIT certification; in time, DEA expects that this certification (or a similar certification) will replace the third-party audit, further reducing their costs.

Based on the above analysis, DEA has determined that although the rule will impact a substantial number of small entities, it will not impose a significant economic impact on any small entity directly subject to the rule.

D. Congressional Review Act

It has been determined that this rule is a major rule as defined by Section 804 of the Small Business Regulatory Enforcement Fairness Act of 1996 (Congressional Review Act). This rule is voluntary and could result in a net reduction in costs. This rule will not result in a major increase in costs or prices; or significant adverse effects on competition,

[65] http://www.nacds.org/wmspage.cfm?parm1=507, accessed 6/17/09.

employment, investment, productivity, innovation, or on the ability of United States-based companies to compete with foreign-based companies in domestic and export markets.

E. Paperwork Reduction Act

As part of its NPRM, DEA included a discussion of the hour burdens associated with the proposed rule. DEA did not receive any comments specific to the information collection aspects of the NPRM.

The Department of Justice, Drug Enforcement Administration, has submitted the following information collection request to the Office of Management and Budget for review and clearance in accordance with review procedures of the Paperwork Reduction Act of 1995.

All suggestions or questions regarding additional information, to include obtaining a copy of the information collection instrument with instructions, should be directed to Mark W. Caverly, Chief, Liaison and Policy Section, Office of Diversion Control, Drug Enforcement Administration, 8701 Morrissette Drive, Springfield, VA 22152.

Overview of information collection 1117-0049:

(1) Type of Information Collection: new collection.

(2) Title of the Form/Collection: Recordkeeping for electronic prescriptions for controlled substances.

(3) Agency form number, if any, and the applicable component of the Department of Justice sponsoring the collection:

Form number: None.

Office of Diversion Control, Drug Enforcement Administration, Department of Justice.

(4) Affected public who will be asked or required to respond, as well as a brief abstract:

Primary: business or other for-profit.

Other: non-profit healthcare facilities.

Abstract: DEA is requiring that each registered practitioner apply to a credential service provider approved by the Federal government to obtain identity proofing and a credential. Hospitals and other institutional practitioners may conduct this process in-house as part of their credentialing. For practitioners currently working at or affiliated with a registered hospital or clinic, the hospital/clinic will have to check a government-issued photographic identification. In the future, this will be done when the hospital/clinic issues credentials to new hires or newly affiliated physicians. At practitioner offices, two people will need to enter logical access control data into the electronic prescription application to grant permissions for individual practitioner registrants to approve and sign controlled substance prescriptions. For larger offices (more than two registrants), DEA registrations will be checked prior to granting access. Similarly pharmacies will have to enter permissions for access to prescription records. Finally, practitioners, hospitals/clinics, and pharmacies will have to check security logs periodically to determine if security incidents have occurred.

(5) An estimate of the total number of respondents and the amount of time estimated for an average respondent to respond:

DEA estimates in the first three years of implementation 217,740 practitioners, 8,688 hospitals and clinics, and 65,421 pharmacies will adopt electronic prescribing for a total of 291,849 respondents. The average practitioner is expected to spend 0.17 hours, the average hospital or clinic, 2.23 hours, and the average pharmacy 0.36 hours annually or an average across all respondents of 0.27 hours per year. Table 14 presents the burden hours by activity, registrant type, and year.

Table 14: Burden Hours by Activity, Registrant Type, and Year

Year 1	**Practitioner**	**Hospitals**	**Pharmacies**	**Total Hours**
Application	5,827			5,827
Registration check	264			264
Access control	1,826		5,452	7,277
Security log	6,086	6,206	21,807	34,099
ID check		27,712		27,712
Total	**14,003**	**33,918**	**27,259**	**75,180**
Year 2	**Practitioner**	**Hospitals**	**Pharmacies**	**Total Hours**
Application	10,004			10,004
Registration check	454			454
Access control	3,101			3,101
Security log	16,423	12,412	21,807	50,642
ID check		28,887		28,887
Total	**29,983**	**41,299**	**21,807**	**93,089**
Year 3	**Practitioner**	**Hospitals**	**Pharmacies**	**Total Hours**
Application	20,459			20,459
Registration check	931			931
Access control	6,292		0	6,292
Security log	37,395	9,120	21,807	68,322
ID check		24,319		24,319
Total	**65,076**	**41,696**	**21,807**	**128,579**

(6) An estimate of the total public burden (in hours) associated with the collection:

The three year burden hours are estimated to be 296,848 or 98,949 hours annually.

If additional information is required contact: Lynn Bryant, Department Clearance Officer, Information Management and Security Staff, Justice Management Division, Department of Justice, Patrick Henry Building, Suite 1600, 601 D Street NW., Washington, DC 20530.

F. Executive Order 12988

This regulation meets the applicable standards set forth in Sections 3(a) and 3(b)(2) of Executive Order 12988 Civil Justice Reform.

G. Executive Order 13132

This rulemaking does not preempt or modify any provision of State law; nor does it impose enforcement responsibilities on any State; nor does it diminish the power of any State to enforce its own laws. Accordingly, this rulemaking does not have federalism implications warranting the application of Executive Order 13132.

H. Unfunded Mandates Reform Act of 1995

This rule will not result in the net expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $120,000,000 or more (adjusted for inflation) in any one year and will not significantly or uniquely affect small governments. Because this rule will not affect other governments, no actions were deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

The economic impact on private entities is analyzed in the Economic Impact Analysis of the Electronic Prescription Rule.

List of Subjects

21 CFR Part 1300

Chemicals, Drug traffic control.

21 CFR Part 1304

Drug traffic control, Reporting and recordkeeping requirements

21 CFR Part 1306

Drug traffic control, Prescription drugs

21 CFR Part 1311

Administrative practice and procedure, Certification authorities, Controlled substances, Digital certificates, Drug traffic control, Electronic signatures, Incorporation by reference, Prescription drugs, Reporting and recordkeeping requirements

For the reasons set out above, 21 CFR parts 1300, 1304, 1306, and 1311 are amended as follows:

PART 1300 – DEFINITIONS

1. The authority citation for part 1300 continues to read as follows:

AUTHORITY: 21 U.S.C. 802, 821, 829, 871(b), 951, 958(f).

2. Section 1300.03 is added to read as follows:

§ 1300.03 Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.

For the purposes of this chapter, the following terms shall have the meanings specified:

Application service provider means an entity that sells electronic prescription or pharmacy applications as a hosted service, where the entity controls access to the application and maintains the software and records on its servers.

Audit trail means a record showing who has accessed an information technology application and what operations the user performed during a given period.

Authentication means verifying the identity of the user as a prerequisite to allowing access to the information application.

Authentication protocol means a well specified message exchange process that verifies possession of a token to remotely authenticate a person to an application.

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable.

Biometric subsystem means the hardware and software used to capture, store, and compare biometric data. The biometric subsystem may be part of a larger application. The biometric subsystem is an automated system capable of:

(1) Capturing a biometric sample from an end user.

(2) Extracting and processing the biometric data from that sample.

(3) Storing the extracted information in a database.

(4) Comparing the biometric data with data contained in one or more reference databases.

(5) Determining how well the stored data matches the newly captured data and indicating whether an identification or verification of identity has been achieved.

Cache means to download and store information on a local server or hard drive.

Certificate policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate revocation list (CRL) means a list of revoked, but unexpired certificates issued by a certification authority.

Certification authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

Certified information systems auditor (CISA) means an individual who has been certified by the Information Systems Audit and Control Association as qualified to audit information systems and who performs compliance audits as a regular ongoing business activity.

Credential means an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Credential service provider (CSP) means a trusted entity that issues or registers tokens and issues electronic credentials to individuals. The CSP may be an independent third party or may issue credentials for its own use.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum--

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the certification authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Digitally sign means to affix a digital signature to a data file.

Electronic prescription means a prescription that is generated on an electronic application and transmitted as an electronic data file.

Electronic prescription application provider means an entity that develops or markets electronic prescription software either as a stand-alone application or as a module in an electronic health record application.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

False match rate means the rate at which an impostor's biometric is falsely accepted as being that of an authorized user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false accept (or acceptance) rate.

False non-match rate means the rate at which a genuine user's biometric is falsely rejected when the user's biometric data fail to match the enrolled data for the user. It is

one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false reject (or rejection) rate, except that it does not include the rate at which a biometric system fails to acquire a biometric sample from a genuine user.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in § 1311.08 of this chapter, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140-2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Security Requirements for Cryptographic Modules," a Federal standard for security requirements for cryptographic modules.

FIPS 180-2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Secure Hash Standard," a Federal secure hash standard.

FIPS 180-3, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Secure Hash Standard (SHS)," a Federal secure hash standard.

FIPS 186-2, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Digital Signature Standard," a Federal standard for applications used to generate and rely upon digital signatures.

FIPS 186-3, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Digital Signature Standard (DSS)," a Federal standard for applications used to generate and rely upon digital signatures.

Hard token means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card, USB drive, one-time password device) rather than on a general purpose computer.

Identity proofing means the process by which a credential service provider or certification authority validates sufficient information to uniquely identify a person.

Installed electronic prescription application means software that is used to create electronic prescriptions and that is installed on a practitioner's computers and servers, where access and records are controlled by the practitioner.

Installed pharmacy application means software that is used to process prescription information and that is installed on a pharmacy's computers or servers and is controlled by the pharmacy.

Intermediary means any technology system that receives and transmits an electronic prescription between the practitioner and pharmacy.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

NIST SP 800-63-1, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Electronic Authentication Guideline," a Federal standard for electronic authentication.

NIST SP 800-76-1, as incorporated by reference in § 1311.08 of this chapter, means the National Institute of Standards and Technology publication entitled "Biometric Data Specification for Personal Identity Verification," a Federal standard for biometric data specifications for personal identity verification.

Operating point means a point chosen on a receiver operating characteristic (ROC) curve for a specific algorithm at which the biometric system is set to function. It is defined by its corresponding coordinates – a false match rate and a false non-match rate. An ROC curve shows graphically the trade-off between the principal two types of errors (false match rate and false non-match rate) of a biometric system by plotting the performance of a specific algorithm on a specific set of data.

Paper prescription means a prescription created on paper or computer generated to be printed or transmitted via facsimile that meets the requirements of part 1306 of this chapter including a manual signature.

Password means a secret, typically a character string (letters, numbers, and other symbols), that a person memorizes and uses to authenticate his identity.

PDA means a Personal Digital Assistant, a handheld computer used to manage contacts, appointments, and tasks.

Pharmacy application provider means an entity that develops or markets software that manages the receipt and processing of electronic prescriptions.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certificate revocation list.

Readily retrievable means that certain records are kept by automatic data processing applications or other electronic or mechanized recordkeeping systems in such a manner that they can be separated out from all other records in a reasonable time and/or records are kept on which certain items are asterisked, redlined, or in some other manner visually identifiable apart from other items appearing on the records.

SAS 70 Audit means a third-party audit of a technology provider that meets the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 70 criteria.

Signing function means any keystroke or other action used to indicate that the practitioner has authorized for transmission and dispensing a controlled substance prescription. The signing function may occur simultaneously with or after the completion of the two-factor authentication protocol that meets the requirements of part 1311 of this chapter. The signing function may have different names (e.g., approve, sign, transmit), but it serves as the practitioner's final authorization that he intends to issue the prescription for a legitimate medical reason in the normal course of his professional practice.

SysTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of electronic systems.

Third-party audit means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Token means something a person possesses and controls (typically a key or password) used to authenticate the person's identity.

Trusted agent means an entity authorized to act as a representative of a certification authority or credential service provider in confirming practitioner identification during the enrollment process.

Valid prescription means a prescription that is issued for a legitimate medical purpose by an individual practitioner licensed by law to administer and prescribe the drugs concerned and acting in the usual course of the practitioner's professional practice.

WebTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of Web sites.

PART 1304 – RECORDS AND REPORTS OF REGISTRANTS

3. The authority citation for part 1304 continues to read as follows:

AUTHORITY: 21 U.S.C. 821, 827, 831, 871(b), 958(e), 965, unless otherwise noted.

4. Section 1304.03 is amended by revising paragraph (c) and adding paragraph (h) to read as follows.

§ 1304.03 Persons required to keep records and file reports.

* * * * *

(c) Except as provided in § 1304.06, a registered individual practitioner is not required to keep records of controlled substances in Schedules II, III, IV, and V that are prescribed in the lawful course of professional practice, unless such substances are prescribed in the course of maintenance or detoxification treatment of an individual.

* * * * *

(h) A person is required to keep the records and file the reports specified in § 1304.06 and part 1311 of this chapter if they are either of the following:

(1) An electronic prescription application provider.

(2) An electronic pharmacy application provider.

5. Section 1304.04 is amended by revising paragraph (b) introductory text, paragraph (b)(1), and paragraph (h) to read as follows:

§ 1304.04 Maintenance of records and inventories.

* * * * *

(b) All registrants that are authorized to maintain a central recordkeeping system under paragraph (a) of this section shall be subject to the following conditions:

(1) The records to be maintained at the central record location shall not include executed order forms and inventories, which shall be maintained at each registered location.

* * * * *

(h) Each registered pharmacy shall maintain the inventories and records of controlled substances as follows:

(1) Inventories and records of all controlled substances listed in Schedule I and II shall be maintained separately from all other records of the pharmacy.

(2) Paper prescriptions for Schedule II controlled substances shall be maintained at the registered location in a separate prescription file.

(3) Inventories and records of Schedules III, IV, and V controlled substances shall be maintained either separately from all other records of the pharmacy or in such form that the information required is readily retrievable from ordinary business records of the pharmacy.

(4) Paper prescriptions for Schedules III, IV, and V controlled substances shall be maintained at the registered location either in a separate prescription file for Schedules III, IV, and V controlled substances only or in such form that they are readily retrievable from the other prescription records of the pharmacy. Prescriptions will be deemed readily retrievable if, at the time they are initially filed, the face of the prescription is stamped in red ink in the lower right corner with the letter “C” no less than 1 inch high and filed either in the prescription file for controlled substances listed in Schedules I and II or in the usual consecutively numbered prescription file for noncontrolled substances. However, if a pharmacy employs a computer application for prescriptions that permits identification by prescription number and retrieval of original documents by prescriber name, patient's name, drug dispensed, and date filled, then the requirement to mark the hard copy prescription with a red “C” is waived.

(5) Records of electronic prescriptions for controlled substances shall be maintained in an application that meets the requirements of part 1311 of this chapter. The computers on which the records are maintained may be located at another location,

but the records must be readily retrievable at the registered location if requested by the Administration or other law enforcement agent. The electronic application must be capable of printing out or transferring the records in a format that is readily understandable to an Administration or other law enforcement agent at the registered location. Electronic copies of prescription records must be sortable by prescriber name, patient name, drug dispensed, and date filled.

6. Section 1304.06 is added to read as follows:

§ 1304.06 Records and reports for electronic prescriptions.

(a) As required by § 1311.120 of this chapter, a practitioner who issues electronic prescriptions for controlled substances must use an electronic prescription application that retains the following information:

(1) The digitally signed record of the information specified in part 1306 of this chapter.

(2) The internal audit trail and any auditable event identified by the internal audit as required by § 1311.150 of this chapter.

(b) An institutional practitioner must retain a record of identity proofing and issuance of the two-factor authentication credential, where applicable, as required by § 1311.110 of this chapter.

(c) As required by § 1311.205 of this chapter, a pharmacy that processes electronic prescriptions for controlled substances must use an application that retains the following:

(1) All of the information required under § 1304.22(c) and part 1306 of this chapter.

(2) The digitally signed record of the prescription as received as required by § 1311.210 of this chapter.

(3) The internal audit trail and any auditable event identified by the internal audit as required by § 1311.215 of this chapter.

(d) A registrant and application service provider must retain a copy of any security incident report filed with the Administration pursuant to §§ 1311.150 and 1311.215 of this chapter.

(e) An electronic prescription or pharmacy application provider must retain third party audit or certification reports as required by § 1311.300 of this chapter.

(f) An application provider must retain a copy of any notification to the Administration regarding an adverse audit or certification report filed with the Administration on problems identified by the third-party audit or certification as required by § 1311.300 of this chapter.

(g) Unless otherwise specified, records and reports must be retained for two years.

PART 1306 – PRESCRIPTIONS

7. The authority citation for part 1306 continues to read as follows:

AUTHORITY: 21 U.S.C. 821, 829, 831, 871(b), unless otherwise noted.

8. Section 1306.05 is revised to read as follows:

§ 1306.05 Manner of issuance of prescriptions.

(a) All prescriptions for controlled substances shall be dated as of, and signed on, the day when issued and shall bear the full name and address of the patient, the drug name, strength, dosage form, quantity prescribed, directions for use, and the name, address and registration number of the practitioner.

(b) A prescription for a Schedule III, IV, or V narcotic drug approved by FDA specifically for "detoxification treatment" or "maintenance treatment" must include the identification number issued by the Administrator under § 1301.28(d) of this chapter or a written notice stating that the practitioner is acting under the good faith exception of § 1301.28(e) of this chapter.

(c) Where a prescription is for gamma-hydroxybutyric acid, the practitioner shall note on the face of the prescription the medical need of the patient for the prescription.

(d) A practitioner may sign a paper prescription in the same manner as he would sign a check or legal document (e.g., J.H. Smith or John H. Smith). Where an oral order is not permitted, paper prescriptions shall be written with ink or indelible pencil, typewriter, or printed on a computer printer and shall be manually signed by the practitioner. A computer-generated prescription that is printed out or faxed by the practitioner must be manually signed.

(e) Electronic prescriptions shall be created and signed using an application that meets the requirements of part 1311 of this chapter.

(f) A prescription may be prepared by the secretary or agent for the signature of a practitioner, but the prescribing practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations. A corresponding liability rests upon the pharmacist, including a pharmacist employed by a central fill pharmacy, who fills a prescription not prepared in the form prescribed by DEA regulations.

(g) An individual practitioner exempted from registration under § 1301.22(c) of this chapter shall include on all prescriptions issued by him the registration number of the hospital or other institution and the special internal code number assigned to him by the

hospital or other institution as provided in § 1301.22(c) of this chapter, in lieu of the registration number of the practitioner required by this section. Each paper prescription shall have the name of the practitioner stamped, typed, or handprinted on it, as well as the signature of the practitioner.

(h) An official exempted from registration under § 1301.23(a) of this chapter must include on all prescriptions issued by him his branch of service or agency (e.g., "U.S. Army" or "Public Health Service") and his service identification number, in lieu of the registration number of the practitioner required by this section. The service identification number for a Public Health Service employee is his Social Security identification number. Each paper prescription shall have the name of the officer stamped, typed, or handprinted on it, as well as the signature of the officer.

9. Section 1306.08 is added to read as follows:

§ 1306.08 Electronic prescriptions.

(a) An individual practitioner may sign and transmit electronic prescriptions for controlled substances provided the practitioner meets all of the following requirements:

(1) The practitioner must comply with all other requirements for issuing controlled substance prescriptions in this part;

(2) The practitioner must use an application that meets the requirements of part 1311 of this chapter; and

(3) The practitioner must comply with the requirements for practitioners in part 1311 of this chapter.

(b) A pharmacy may fill an electronically transmitted prescription for a controlled substance provided the pharmacy complies with all other requirements for filling

controlled substance prescriptions in this part and with the requirements of part 1311 of this chapter.

(c) To annotate an electronic prescription, a pharmacist must include all of the information that this part requires in the prescription record.

(d) If the content of any of the information required under § 1306.05 for a controlled substance prescription is altered during the transmission, the prescription is deemed to be invalid and the pharmacy may not dispense the controlled substance.

10. In § 1306.11, paragraphs (a), (c), (d)(1), and (d)(4) are revised to read as follows:

§ 1306.11 Requirement of prescription.

(a) A pharmacist may dispense directly a controlled substance listed in Schedule II that is a prescription drug as determined under section 503 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 353(b)) only pursuant to a written prescription signed by the practitioner, except as provided in paragraph (d) of this section. A paper prescription for a Schedule II controlled substance may be transmitted by the practitioner or the practitioner's agent to a pharmacy via facsimile equipment, provided that the original manually signed prescription is presented to the pharmacist for review prior to the actual dispensing of the controlled substance, except as noted in paragraph (e), (f), or (g) of this section. The original prescription shall be maintained in accordance with § 1304.04(h) of this chapter.

* * * * *

(c) An institutional practitioner may administer or dispense directly (but not prescribe) a controlled substance listed in Schedule II only pursuant to a written prescription signed by the prescribing individual practitioner or to an order for

medication made by an individual practitioner that is dispensed for immediate administration to the ultimate user.

(d) * * *

(1) The quantity prescribed and dispensed is limited to the amount adequate to treat the patient during the emergency period (dispensing beyond the emergency period must be pursuant to a paper or electronic prescription signed by the prescribing individual practitioner);

* * * * *

(4) Within 7 days after authorizing an emergency oral prescription, the prescribing individual practitioner shall cause a written prescription for the emergency quantity prescribed to be delivered to the dispensing pharmacist. In addition to conforming to the requirements of § 1306.05, the prescription shall have written on its face "Authorization for Emergency Dispensing," and the date of the oral order. The paper prescription may be delivered to the pharmacist in person or by mail, but if delivered by mail it must be postmarked within the 7-day period. Upon receipt, the dispensing pharmacist must attach this paper prescription to the oral emergency prescription that had earlier been reduced to writing. For electronic prescriptions, the pharmacist must annotate the record of the electronic prescription with the original authorization and date of the oral order. The pharmacist must notify the nearest office of the Administration if the prescribing individual practitioner fails to deliver a written prescription to him; failure of the pharmacist to do so shall void the authority conferred by this paragraph to dispense without a written prescription of a prescribing individual practitioner.

* * * * *

11. In § 1306.13, paragraph (a) is revised to read as follows:

§ 1306.13 Partial filling of prescriptions.

(a) The partial filling of a prescription for a controlled substance listed in Schedule II is permissible if the pharmacist is unable to supply the full quantity called for in a written or emergency oral prescription and he makes a notation of the quantity supplied on the face of the written prescription, written record of the emergency oral prescription, or in the electronic prescription record. The remaining portion of the prescription may be filled within 72 hours of the first partial filling; however, if the remaining portion is not or cannot be filled within the 72-hour period, the pharmacist shall notify the prescribing individual practitioner. No further quantity may be supplied beyond 72 hours without a new prescription.

* * * * *

12. In § 1306.15, paragraph (a)(1) is revised to read as follows:

§ 1306.15 Provision of prescription information between retail pharmacies and central fill pharmacies for prescriptions of Schedule II controlled substances.

* * * * *

(a) * * *

(1) Write the words “CENTRAL FILL” on the face of the original paper prescription and record the name, address, and DEA registration number of the central fill pharmacy to which the prescription has been transmitted, the name of the retail pharmacy pharmacist transmitting the prescription, and the date of transmittal. For electronic prescriptions the name, address, and DEA registration number of the central fill

pharmacy to which the prescription has been transmitted, the name of the retail pharmacy pharmacist transmitting the prescription, and the date of transmittal must be added to the electronic prescription record.

* * * * *

13. In § 1306.21, paragraphs (a) and (c) are revised to read as follows:

§ 1306.21 Requirement of prescription.

(a) A pharmacist may dispense directly a controlled substance listed in Schedule III, IV, or V that is a prescription drug as determined under section 503(b) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 353(b)) only pursuant to either a paper prescription signed by a practitioner, a facsimile of a signed paper prescription transmitted by the practitioner or the practitioner's agent to the pharmacy, an electronic prescription that meets the requirements of this part and part 1311 of this chapter, or an oral prescription made by an individual practitioner and promptly reduced to writing by the pharmacist containing all information required in § 1306.05, except for the signature of the practitioner.

* * * * *

(c) An institutional practitioner may administer or dispense directly (but not prescribe) a controlled substance listed in Schedule III, IV, or V only pursuant to a paper prescription signed by an individual practitioner, a facsimile of a paper prescription or order for medication transmitted by the practitioner or the practitioner's agent to the institutional practitioner-pharmacist, an electronic prescription that meets the requirements of this part and part 1311 of this chapter, or an oral prescription made by an individual practitioner and promptly reduced to writing by the pharmacist (containing all

information required in § 1306.05 except for the signature of the individual practitioner), or pursuant to an order for medication made by an individual practitioner that is dispensed for immediate administration to the ultimate user, subject to § 1306.07.

14. Section 1306.22 is revised to read as follows:

§ 1306.22 Refilling of prescriptions.

(a) No prescription for a controlled substance listed in Schedule III or IV shall be filled or refilled more than six months after the date on which such prescription was issued. No prescription for a controlled substance listed in Schedule III or IV authorized to be refilled may be refilled more than five times.

(b) Each refilling of a prescription shall be entered on the back of the prescription or on another appropriate document or electronic prescription record. If entered on another document, such as a medication record, or electronic prescription record, the document or record must be uniformly maintained and readily retrievable.

(c) The following information must be retrievable by the prescription number:

(1) The name and dosage form of the controlled substance.

(2) The date filled or refilled.

(3) The quantity dispensed.

(4) The initials of the dispensing pharmacist for each refill.

(5) The total number of refills for that prescription.

(d) If the pharmacist merely initials and dates the back of the prescription or annotates the electronic prescription record, it shall be deemed that the full face amount of the prescription has been dispensed.

(e) The prescribing practitioner may authorize additional refills of Schedule III or IV controlled substances on the original prescription through an oral refill authorization transmitted to the pharmacist provided the following conditions are met:

(1) The total quantity authorized, including the amount of the original prescription, does not exceed five refills nor extend beyond six months from the date of issue of the original prescription.

(2) The pharmacist obtaining the oral authorization records on the reverse of the original paper prescription or annotates the electronic prescription record with the date, quantity of refill, number of additional refills authorized, and initials the paper prescription or annotates the electronic prescription record showing who received the authorization from the prescribing practitioner who issued the original prescription.

(3) The quantity of each additional refill authorized is equal to or less than the quantity authorized for the initial filling of the original prescription.

(4) The prescribing practitioner must execute a new and separate prescription for any additional quantities beyond the five-refill, six-month limitation.

(f) As an alternative to the procedures provided by paragraphs (a) through (e) of this section, a computer application may be used for the storage and retrieval of refill information for original paper prescription orders for controlled substances in Schedule III and IV, subject to the following conditions:

(1) Any such proposed computerized application must provide online retrieval (via computer monitor or hard-copy printout) of original prescription order information for those prescription orders that are currently authorized for refilling. This shall include, but is not limited to, data such as the original prescription number; date of issuance of the

original prescription order by the practitioner; full name and address of the patient; name, address, and DEA registration number of the practitioner; and the name, strength, dosage form, quantity of the controlled substance prescribed (and quantity dispensed if different from the quantity prescribed), and the total number of refills authorized by the prescribing practitioner.

(2) Any such proposed computerized application must also provide online retrieval (via computer monitor or hard-copy printout) of the current refill history for Schedule III or IV controlled substance prescription orders (those authorized for refill during the past six months.) This refill history shall include, but is not limited to, the name of the controlled substance, the date of refill, the quantity dispensed, the identification code, or name or initials of the dispensing pharmacist for each refill and the total number of refills dispensed to date for that prescription order.

(3) Documentation of the fact that the refill information entered into the computer each time a pharmacist refills an original paper, fax, or oral prescription order for a Schedule III or IV controlled substance is correct must be provided by the individual pharmacist who makes use of such an application. If such an application provides a hard-copy printout of each day's controlled substance prescription order refill data, that printout shall be verified, dated, and signed by the individual pharmacist who refilled such a prescription order. The individual pharmacist must verify that the data indicated are correct and then sign this document in the same manner as he would sign a check or legal document (e.g., J.H. Smith, or John H. Smith). This document shall be maintained in a separate file at that pharmacy for a period of two years from the dispensing date. This printout of the day's controlled substance prescription order refill data must be

provided to each pharmacy using such a computerized application within 72 hours of the date on which the refill was dispensed. It must be verified and signed by each pharmacist who is involved with such dispensing. In lieu of such a printout, the pharmacy shall maintain a bound log book, or separate file, in which each individual pharmacist involved in such dispensing shall sign a statement (in the manner previously described) each day, attesting to the fact that the refill information entered into the computer that day has been reviewed by him and is correct as shown. Such a book or file must be maintained at the pharmacy employing such an application for a period of two years after the date of dispensing the appropriately authorized refill.

(4) Any such computerized application shall have the capability of producing a printout of any refill data that the user pharmacy is responsible for maintaining under the Act and its implementing regulations. For example, this would include a refill-by-refill audit trail for any specified strength and dosage form of any controlled substance (by either brand or generic name or both). Such a printout must include name of the prescribing practitioner, name and address of the patient, quantity dispensed on each refill, date of dispensing for each refill, name or identification code of the dispensing pharmacist, and the number of the original prescription order. In any computerized application employed by a user pharmacy the central recordkeeping location must be capable of sending the printout to the pharmacy within 48 hours, and if a DEA Special Agent or Diversion Investigator requests a copy of such printout from the user pharmacy, it must, if requested to do so by the Agent or Investigator, verify the printout transmittal capability of its application by documentation (e.g., postmark).

(5) In the event that a pharmacy which employs such a computerized application experiences system down-time, the pharmacy must have an auxiliary procedure which will be used for documentation of refills of Schedule III and IV controlled substance prescription orders. This auxiliary procedure must ensure that refills are authorized by the original prescription order, that the maximum number of refills has not been exceeded, and that all of the appropriate data are retained for online data entry as soon as the computer system is available for use again.

(g) When filing refill information for original paper, fax, or oral prescription orders for Schedule III or IV controlled substances, a pharmacy may use only one of the two applications described in paragraphs (a) through (e) or (f) of this section.

(h) When filing refill information for electronic prescriptions, a pharmacy must use an application that meets the requirements of part 1311 of this chapter.

15. Section 1306.25 is revised to read as follows:

§ 1306.25 Transfer between pharmacies of prescription information for Schedules III, IV, and V controlled substances for refill purposes.

(a) The transfer of original prescription information for a controlled substance listed in Schedule III, IV, or V for the purpose of refill dispensing is permissible between pharmacies on a one-time basis only. However, pharmacies electronically sharing a real-time, online database may transfer up to the maximum refills permitted by law and the prescriber's authorization.

(b) Transfers are subject to the following requirements:

(1) The transfer must be communicated directly between two licensed pharmacists.

(2) The transferring pharmacist must do the following:

(i) Write the word "VOID" on the face of the invalidated prescription; for electronic prescriptions, information that the prescription has been transferred must be added to the prescription record.

(ii) Record on the reverse of the invalidated prescription the name, address, and DEA registration number of the pharmacy to which it was transferred and the name of the pharmacist receiving the prescription information; for electronic prescriptions, such information must be added to the prescription record.

(iii) Record the date of the transfer and the name of the pharmacist transferring the information.

(3) For paper prescriptions and prescriptions received orally and reduced to writing by the pharmacist pursuant to § 1306.21(a), the pharmacist receiving the transferred prescription information must write the word "transfer" on the face of the transferred prescription and reduce to writing all information required to be on a prescription pursuant to § 1306.05 and include:

(i) Date of issuance of original prescription.

(ii) Original number of refills authorized on original prescription.

(iii) Date of original dispensing.

(iv) Number of valid refills remaining and date(s) and locations of previous refill(s).

(v) Pharmacy's name, address, DEA registration number, and prescription number from which the prescription information was transferred.

(vi) Name of pharmacist who transferred the prescription.

(vii) Pharmacy's name, address, DEA registration number, and prescription number from which the prescription was originally filled.

(4) For electronic prescriptions being transferred electronically, the transferring pharmacist must provide the receiving pharmacist with the following information in addition to the original electronic prescription data:

(i) The date of the original dispensing.

(ii) The number of refills remaining and the date(s) and locations of previous refills.

(iii) The transferring pharmacy's name, address, DEA registration number, and prescription number for each dispensing.

(iv) The name of the pharmacist transferring the prescription.

(v) The name, address, DEA registration number, and prescription number from the pharmacy that originally filled the prescription, if different.

(5) The pharmacist receiving a transferred electronic prescription must create an electronic record for the prescription that includes the receiving pharmacist’s name and all of the information transferred with the prescription under paragraph (b)(4) of this section.

(c) The original and transferred prescription(s) must be maintained for a period of two years from the date of last refill.

(d) Pharmacies electronically accessing the same prescription record must satisfy all information requirements of a manual mode for prescription transferal.

(e) The procedure allowing the transfer of prescription information for refill purposes is permissible only if allowable under existing State or other applicable law.

PART 1311 – REQUIREMENTS FOR ELECTRONIC ORDERS AND PRESCRIPTIONS

16. The authority citation for part 1311 continues to read as follows:

AUTHORITY: 21 U.S.C. 821, 828, 829, 871(b), 958(e), 965, unless otherwise noted.

17. The heading for part 1311 is revised to read as set forth above.

18. Section 1311.01 is revised to read as follows:

§ 1311.01 Scope.

This part sets forth the rules governing the creation, transmission, and storage of electronic orders and prescriptions.

19. Section 1311.02 is revised to read as follows:

§ 1311.02 Definitions.

Any term contained in this part shall have the definition set forth in section 102 of the Act (21 U.S.C. 802) or part 1300 of this chapter.

20. § 1311.08 is revised to read as follows:

§ 1311.08 Incorporation by reference.

(a) These incorporations by reference were approved by the Director of the Federal Register in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. Copies may be inspected at the Drug Enforcement Administration, 600 Army Navy Drive, Arlington, VA 22202 or at the National Archives and Records Administration (NARA). For information on the availability of this material at the Drug Enforcement Administration, call (202) 307-1000. For information on the availability of this material at NARA, call

(202) 741-6030 or go to:

http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html.

(b) These standards are available from the National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899-8930, (301) 975-6478 or TTY (301) 975-8295, inquiries@nist.gov, and are available at http://csrc.nist.gov/ . The following standards are incorporated by reference:

(1) Federal Information Processing Standard Publication (FIPS PUB) 140-2, Change Notices (12-03-2002), Security Requirements for Cryptographic Modules, May 25, 2001 (FIPS 140-2) including Annexes A through D; incorporation by reference approved for §§ 1311.30(b), 1311.55(b), 1311.115(b), 1311.120(b), 1311.205(b).

(i) Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, September 23, 2004.

(ii) Annex B: Approved Protection Profiles for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, November 4, 2004.

(iii) Annex C: Approved Random Number Generators for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, January 31, 2005.

(iv) Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, February 23, 2004.

(2) Federal Information Processing Standard Publication (FIPS PUB) 180-2, Secure Hash Standard, August 1, 2002, as amended by change notice 1, February 25, 2004 (FIPS 180-2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(3) Federal Information Processing Standard Publication (FIPS PUB) 180-3, Secure Hash Standard (SHS), October 2008 (FIPS 180-3); incorporation by reference approved for §§ 1311.120(b) and 1311.205(b).

(4) Federal Information Processing Standard Publication (FIPS PUB) 186-2, Digital Signature Standard, January 27, 2000, as amended by Change Notice 1, October 5, 2001 (FIPS 186-2); incorporation by reference approved for §§ 1311.30(b) and 1311.55(b).

(5) Federal Information Processing Standard Publication (FIPS PUB) 186-3, Digital Signature Standard (DSS), June 2009 (FIPS 186-3); incorporation by reference approved for §§ 1311.120(b), 1311.205(b), and 1311.210(c).

(6) Draft NIST Special Publication 800-63-1, Electronic Authentication Guideline, December 8, 2008 (NIST SP 800-63-1); Burr, W. et al; incorporation by reference approved for § 1311.105(a).

(7) NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007 (NIST SP 800-76-1); Wilson, C. et al; incorporation by reference approved for § 1311.116(d).

21. Subpart C, consisting of §§1311.100 through 1311.305, is added to read as follows:

Subpart C – Electronic Prescriptions

Sec.

Subpart C – Electronic Prescriptions

§ 1311.100 General.

(a) This subpart addresses the requirements that must be met to issue and process Schedule II, III, IV, and V controlled substance prescriptions electronically.

(b) A practitioner may issue a prescription for a Schedule II, III, IV, or V controlled substance electronically if all of the following conditions are met:

(1) The practitioner is registered as an individual practitioner or exempt from the requirement of registration under part 1301 of this chapter and is authorized under the registration or exemption to dispense the controlled substance;

(2) The practitioner uses an electronic prescription application that meets all of the applicable requirements of this subpart; and

(3) The prescription is otherwise in conformity with the requirements of the Act and this chapter.

(c) An electronic prescription for a Schedule II, III, IV, or V controlled substance created using an electronic prescription application that does not meet the requirements of this subpart is not a valid prescription, as that term is defined in § 1300.03 of this chapter.

(d) A controlled substance prescription created using an electronic prescription application that meets the requirements of this subpart is not a valid prescription if any of the functions required under this subpart were disabled when the prescription was indicated as ready for signature and signed.

(e) A registered pharmacy may process electronic prescriptions for controlled substances only if all of the following conditions are met:

(1) The pharmacy uses a pharmacy application that meets all of the applicable requirements of this subpart; and

(2) The prescription is otherwise in conformity with the requirements of the Act and this chapter.

(f) Nothing in this part alters the responsibilities of the practitioner and pharmacy, specified in part 1306 of this chapter, to ensure the validity of a controlled substance prescription.

§ 1311.102 Practitioner responsibilities.

(a) The practitioner must retain sole possession of the hard token, where applicable, and must not share the password or other knowledge factor, or biometric information, with any other person. The practitioner must not allow any other person to use the token or enter the knowledge factor or other identification means to sign prescriptions for controlled substances. Failure by the practitioner to secure the hard

token, knowledge factor, or biometric information may provide a basis for revocation or suspension of registration pursuant to section 304(a)(4) of the Act (21 U.S.C. 824(a)(4)).

(b) The practitioner must notify the individuals designated under § 1311.125 or § 1311.130 within one business day of discovery that the hard token has been lost, stolen, or compromised or the authentication protocol has been otherwise compromised. A practitioner who fails to comply with this provision may be held responsible for any controlled substance prescriptions written using his two-factor authentication credential.

(c) If the practitioner is notified by an intermediary or pharmacy that an electronic prescription was not successfully delivered, as provided in § 1311.170, he must ensure that any paper or oral prescription (where permitted) issued as a replacement of the original electronic prescription indicates that the prescription was originally transmitted electronically to a particular pharmacy and that the transmission failed.

(d) Before initially using an electronic prescription application to sign and transmit controlled substance prescriptions, the practitioner must determine that the third-party auditor or certification organization has found that the electronic prescription application records, stores, and transmits the following accurately and consistently:

(1) The information required for a prescription under § 1306.05(a) of this chapter.

(2) The indication of signing as required by § 1311.120(b)(17) or the digital signature created by the practitioner's private key.

(3) The number of refills as required by § 1306.22 of this chapter.

(e) If the third-party auditor or certification organization has found that an electronic prescription application does not accurately and consistently record, store, and transmit other information required for prescriptions under this chapter, the practitioner

must not create, sign, and transmit electronic prescriptions for controlled substances that are subject to the additional information requirements.

(f) The practitioner must not use the electronic prescription application to sign and transmit electronic controlled substance prescriptions if any of the functions of the application required by this subpart have been disabled or appear to be functioning improperly.

(g) If an electronic prescription application provider notifies an individual practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies him that the application provider has identified a issue that makes the application non-compliant, the practitioner must do the following:

(1) Immediately cease to issue electronic controlled substance prescriptions using the application.

(2) Ensure, for an installed electronic prescription application at an individual practitioner's practice, that the individuals designated under § 1311.125 terminate access for signing controlled substance prescriptions.

(h) If an electronic prescription application provider notifies an institutional practitioner that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that the application provider has identified a issue that makes the application non-compliant, the institutional practitioner must ensure that the individuals designated under § 1311.130 terminate access for signing controlled substance prescriptions.

(i) An individual practitioner or institutional practitioner that receives a notification that the electronic prescription application is not in compliance with the requirements of this part must not use the application to issue electronic controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(j) The practitioner must notify both the individuals designated under § 1311.125 or § 1311.130 and the Administration within one business day of discovery that one or more prescriptions that were issued under a DEA registration held by that practitioner were prescriptions the practitioner had not signed or were not consistent with the prescriptions he signed.

(k) The practitioner has the same responsibilities when issuing prescriptions for controlled substances via electronic means as when issuing a paper or oral prescription. Nothing in this subpart relieves a practitioner of his responsibility to dispense controlled substances only for a legitimate medical purpose while acting in the usual course of his professional practice. If an agent enters information at the practitioner's direction prior to the practitioner reviewing and approving the information and signing and authorizing the transmission of that information, the practitioner is responsible in case the prescription does not conform in all essential respects to the law and regulations.

§ 1311.105 Requirements for obtaining an authentication credential – Individual practitioners.

(a) An individual practitioner must obtain a two-factor authentication credential from one of the following:

(1) A credential service provider that has been approved by the General Services Administration Office of Technology Strategy/Division of Identity Management to conduct identity proofing that meets the requirements of Assurance Level 3 or above as specified in NIST SP 800-63-1 as incorporated by reference in § 1311.08.

(2) For digital certificates, a certification authority that is cross-certified with the Federal Bridge certification authority and that operates at a Federal Bridge Certification Authority basic assurance level or above.

(b) The practitioner must submit identity proofing information to the credential service provider or certification authority as specified by the credential service provider or certification authority.

(c) The credential service provider or certification authority must issue the authentication credential using two channels (e.g., e-mail, mail, or telephone call). If one of the factors used in the authentication protocol is a biometric, or if the practitioner has a hard token that is being enabled to sign controlled substances prescriptions, the credential service provider or certification authority must issue two pieces of information used to generate or activate the authentication credential using two channels.

§ 1311.110 Requirements for obtaining an authentication credential – Individual practitioners eligible to use an electronic prescription application of an institutional practitioner.

(a) For any registrant or person exempted from the requirement of registration under § 1301.22(c) of this chapter who is eligible to use the institutional practitioner's electronic prescription application to sign prescriptions for controlled substances, the entity within a DEA-registered institutional practitioner that grants that individual

practitioner privileges at the institutional practitioner (e.g., a hospital credentialing office) may conduct identity proofing and authorize the issuance of the authentication credential. That entity must do the following:

(1) Ensure that photographic identification issued by the Federal Government or a State government matches the person presenting the identification.

(2) Ensure that the individual practitioner's State authorization to practice and, where applicable, State authorization to prescribe controlled substances, is current and in good standing.

(3) Either ensure that the individual practitioner's DEA registration is current and in good standing or ensure that the institutional practitioner has granted the individual practitioner exempt from the requirement of registration under § 1301.22 of this chapter privileges to prescribe controlled substances using the institutional practitioner's DEA registration number.

(4) If the individual practitioner is an employee of a health care facility that is operated by the Department of Veterans Affairs, confirm that the individual practitioner has been duly appointed to practice at that facility by the Secretary of the Department of Veterans Affairs pursuant to 38 U.S.C. 7401-7408.

(5) If the individual practitioner is working at a health care facility operated by the Department of Veterans Affairs on a contractual basis pursuant to 38 U.S.C. 8153 and, in the performance of his duties, prescribes controlled substances, confirm that the individual practitioner meets the criteria for eligibility for appointment under 38 U.S.C. 7401-7408 and is prescribing controlled substances under the registration of such facility.

(b) An institutional practitioner that elects to conduct identity proofing must provide authorization to issue the authentication credentials to a separate entity within the institutional practitioner or to an outside credential Service provider or certification authority that meets the requirements of § 1311.105(a).

(c) When an institutional practitioner is conducting identity proofing and submitting information to a credential service provider or certification authority to authorize the issuance of authentication credentials, the institutional practitioner must meet any requirements that the credential service provider or certification authority imposes on entities that serve as trusted agents.

(d) An institutional practitioner that elects to conduct identity proofing and authorize the issuance of the authentication credential as provided in paragraphs (a) through (c) of this section must do so in a manner consistent with the institutional practitioner's general obligation to maintain effective controls against diversion. Failure to meet this obligation may result in remedial action consistent with § 1301.36 of this chapter.

(e) An institutional practitioner that elects to conduct identity proofing must retain a record of the identity-proofing. An institutional practitioner that elects to issue the two-factor authentication credential must retain a record of the issuance of the credential.

§ 1311.115 Additional requirements for two-factor authentication.

(a) To sign a controlled substance prescription, the electronic prescription application must require the practitioner to authenticate to the application using an authentication protocol that uses two of the following three factors:

(1) Something only the practitioner knows, such as a password or response to a challenge question.

(2) Something the practitioner is, biometric data such as a fingerprint or iris scan.

(3) Something the practitioner has, a device (hard token) separate from the computer to which the practitioner is gaining access.

(b) If one factor is a hard token, it must be separate from the computer to which it is gaining access and must meet at least the criteria of FIPS 140-2 Security Level 1, as incorporated by reference in § 1311.08, for cryptographic modules or one-time-password devices.

(c) If one factor is a biometric, the biometric subsystem must comply with the requirements of § 1311.116.

§ 1311.116 Additional requirements for biometrics.

(a) If one of the factors used to authenticate to the electronic prescription application is a biometric as described in § 1311.115, it must comply with the following requirements.

(b) The biometric subsystem must operate at a false match rate of 0.001 or lower.

(c) The biometric subsystem must use matching software that has demonstrated performance at the operating point corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate. Testing to demonstrate performance must be conducted by the National Institute of Standards and Technology or another DEA-approved government or nongovernment laboratory. Such testing must comply with the requirements of paragraph (h) of this section.

(d) The biometric subsystem must conform to Personal Identity Verification authentication biometric acquisition specifications, pursuant to NIST SP 800-76-1 as incorporated by reference in § 1311.08, if they exist for the biometric modality of choice.

(e) The biometric subsystem must either be co-located with a computer or PDA that the practitioner uses to issue electronic prescriptions for controlled substances, where the computer or PDA is located in a known, controlled location, or be built directly into the practitioner's computer or PDA that he uses to issue electronic prescriptions for controlled substances.

(f) The biometric subsystem must store device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication to the electronic prescription application.

(g) The biometric subsystem must protect the biometric data (raw data or templates), match results, and/or non-match results when authentication is not local. If sent over an open network, biometric data (raw data or templates), match results, and/or non-match results must be:

(1) Cryptographically source authenticated;

(2) Combined with a random challenge, a nonce, or a time stamp to prevent replay;

(3) Cryptographically protected for integrity and confidentiality; and

(4) Sent only to authorized systems.

(h) Testing of the biometric subsystem must have the following characteristics:

(1) The test is conducted by a laboratory that does not have an interest in the outcome (positive or negative) of performance of a submission or biometric.

(2) Test data are sequestered.

(3) Algorithms are provided to the testing laboratory (as opposed to scores or other information).

(4) The operating point(s) corresponding with the false match rate described in paragraph (b) of this section, or a lower false match rate, is tested so that there is at least 95% confidence that the false match and non-match rates are equal to or less than the observed value.

(5) Results of the testing are made publicly available.

§ 1311.120 Electronic prescription application requirements.

(a) A practitioner may only use an electronic prescription application that meets the requirements in paragraph (b) of this section to issue electronic controlled substance prescriptions.

(b) The electronic prescription application must meet the requirements of this subpart including the following:

(1) The electronic prescription application must do the following:

(i) Link each registrant, by name, to at least one DEA registration number.

(ii) Link each practitioner exempt from registration under § 1301.22(c) of this chapter to the institutional practitioner's DEA registration number and the specific internal code number required under § 1301.22(c)(5) of this chapter.

(2) The electronic prescription application must be capable of the setting of logical access controls to limit permissions for the following functions:

(i) Indication that a prescription is ready for signing and signing controlled substance prescriptions.

(ii) Creating, updating, and executing the logical access controls for the functions specified in paragraph (b)(2)(i) of this section.

(3) Logical access controls must be set by individual user name or role. If the application sets logical access control by role, it must not allow an individual to be assigned the role of registrant unless that individual is linked to at least one DEA registration number as provided in paragraph (b)(1) of this section.

(4) The application must require that the setting and changing of logical access controls specified under paragraph (b)(2) of this section involve the actions of two individuals as specified in §§ 1311.125 or 1311.130. Except for institutional practitioners, a practitioner authorized to sign controlled substance prescriptions must approve logical access control entries.

(5) The electronic prescription application must accept two-factor authentication that meets the requirements of § 1311.115 and require its use for signing controlled substance prescriptions and for approving data that set or change logical access controls related to reviewing and signing controlled substance prescriptions.

(6) The electronic prescription application must be capable of recording all of the applicable information required in part 1306 of this chapter for the controlled substance prescription.

(7) If a practitioner has more than one DEA registration number, the electronic prescription application must require the practitioner or his agent to select the DEA registration number to be included on the prescription.

(8) The electronic prescription application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The electronic prescription application must present for the practitioner's review and approval all of the following data for each controlled substance prescription:

(i) The date of issuance.

(ii) The full name of the patient.

(iii) The drug name.

(iv) The dosage strength and form, quantity prescribed, and directions for use.

(v) The number of refills authorized, if applicable, for prescriptions for Schedule III, IV, and V controlled substances.

(vi) For prescriptions written in accordance with the requirements of § 1306.12(b) of this chapter, the earliest date on which a pharmacy may fill each prescription.

(vii) The name, address, and DEA registration number of the prescribing practitioner.

(viii) The statement required under § 1311.140(a)(3).

(10) The electronic prescription application must require the prescribing practitioner to indicate that each controlled substance prescription is ready for signing. The electronic prescription application must not permit alteration of the DEA elements after the practitioner has indicated that a controlled substance prescription is ready to be signed without requiring another review and indication of readiness for signing. Any controlled substance prescription not indicated as ready to be signed shall not be signed or transmitted.

(11) While the information required by paragraph (b)(9) of this section and the statement required by § 1311.140(a)(3) remain displayed, the electronic prescription application must prompt the prescribing practitioner to authenticate to the application, using two-factor authentication, as specified in § 1311.140(a)(4), which will constitute the signing of the prescription by the practitioner for purposes of § 1306.05(a) and (e) of this chapter.

(12) The electronic prescription application must not permit a practitioner other than the prescribing practitioner whose DEA number (or institutional practitioner DEA number and extension data for the individual practitioner) is listed on the prescription as the prescribing practitioner and who has indicated that the prescription is ready to be signed to sign the prescription.

(13) Where a practitioner seeks to prescribe more than one controlled substance at one time for a particular patient, the electronic prescription application may allow the practitioner to sign multiple prescriptions for a single patient at one time using a single invocation of the two-factor authentication protocol provided the following has occurred: the practitioner has individually indicated that each controlled substance prescription is ready to be signed while the information required by paragraph (b)(9) of this section for each such prescription is displayed along with the statement required by § 1311.140(a)(3).

(14) The electronic prescription application must time and date stamp the prescription when the signing function is used.

(15) When the practitioner uses his two-factor authentication credential as specified in § 1311.140(a)(4), the electronic prescription application must digitally sign at

least the information required by part 1306 of this chapter and electronically archive the digitally signed record. If the practitioner signs the prescription with his own private key, as provided in § 1311.145, the electronic prescription application must electronically archive a copy of the digitally signed record, but need not apply the application's digital signature to the record.

(16) The digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140-2 Security Level 1 validated. FIPS 140-2 is incorporated by reference in § 1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186-3 and FIPS 180-3, as incorporated by reference in § 1311.08.

(iii) The electronic prescription application's private key must be stored encrypted on a FIPS 140-2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140-2 is incorporated by reference in § 1311.08.

(iv) For software implementations, when the signing module is deactivated, the application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(17) Unless the digital signature created by an individual practitioner's private key is being transmitted to the pharmacy with the prescription, the electronic prescription application must include in the data file transmitted an indication that the prescription was signed by the prescribing practitioner.

(18) The electronic prescription application must not transmit a controlled substance prescription unless the signing function described in § 1311.140(a)(4) has been used.

(19) The electronic prescription application must not allow alteration of any of the information required by part 1306 of this chapter after the prescription has been digitally signed. Any alteration of the information required by part 1306 of this chapter after the prescription is digitally signed must cancel the prescription.

(20) The electronic prescription application must not allow transmission of a prescription that has been printed.

(21) The electronic prescription application must allow printing of a prescription after transmission only if the printed prescription is clearly labeled as a copy not for dispensing. The electronic prescription application may allow printing of prescription information if clearly labeled as being for informational purposes. The electronic prescription application may transfer such prescription information to medical records.

(22) If the transmission of an electronic prescription fails, the electronic prescription application may print the prescription. The prescription must indicate that it was originally transmitted electronically to, and provide the name of, a specific pharmacy, the date and time of transmission, and that the electronic transmission failed.

(23) The electronic prescription application must maintain an audit trail of all actions related to the following:

(i) The creation, alteration, indication of readiness for signing, signing, transmission, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the issuance of controlled substance prescriptions.

(iii) Notification of a failed transmission.

(iv) Auditable events as specified in § 1311.150.

(24) The electronic prescription application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(25) The electronic prescription application must conduct internal audits and generate reports on any of the events specified in § 1311.150 in a format that is readable by the practitioner. Such internal audits may be automated and need not require human intervention to be conducted.

(26) The electronic prescription application must protect the stored audit records from unauthorized deletion. The electronic prescription application shall prevent modifications to the audit records.

(27) The electronic prescription application must do the following:

(i) Generate a log of all controlled substance prescriptions issued by a practitioner during the previous calendar month and provide the log to the practitioner no later than seven calendar days after that month.

(ii) Be capable of generating a log of all controlled substance prescriptions issued by a practitioner for a period specified by the practitioner upon request. Prescription

information available from which to generate the log must span at least the previous two years.

(iii) Archive all logs generated.

(iv) Ensure that all logs are easily readable or easily rendered into a format that a person can read.

(v) Ensure that all logs are sortable by patient name, drug name, and date of issuance of the prescription.

(28) Where the electronic prescription application is required by this part to archive or otherwise maintain records, it must retain such records electronically for two years from the date of the record's creation and comply with all other requirements of § 1311.305.

§ 1311.125 Requirements for establishing logical access control - Individual practitioner.

(a) At each registered location where one or more individual practitioners wish to use an electronic prescription application meeting the requirements of this subpart to issue controlled substance prescriptions, the registrant(s) must designate at least two individuals to manage access control to the application. At least one of the designated individuals must be a registrant who is authorized to issue controlled substance prescriptions and who has obtained a two-factor authentication credential as provided in § 1311.105.

(b) At least one of the individuals designated under paragraph (a) of this section must verify that the DEA registration and State authorization(s) to practice and, where applicable, State authorization(s) to dispense controlled substances of each registrant

being granted permission to sign electronic prescriptions for controlled substances are current and in good standing.

(c) After one individual designated under paragraph (a) of this section enters data that grants permission for individual practitioners to have access to the prescription functions that indicate readiness for signature and signing or revokes such authorization, a second individual designated under paragraph (a) of this section must use his two-factor authentication credential to satisfy the logical access controls. The second individual must be a DEA registrant.

(d) A registrant's permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) A hard token or any other authentication factor required by the two-factor authentication protocol is lost, stolen, or compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) The individual practitioner is no longer authorized to use the electronic prescription application (e.g., when the individual practitioner leaves the practice).

§ 1311.130 Requirements for establishing logical access control - Institutional practitioner.

(a) The entity within an institutional practitioner that conducts the identity proofing under § 1311.110 must develop a list of individual practitioners who are permitted to use the institutional practitioner's electronic prescription application to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. The list must be approved by two individuals.

(b) After the list is approved, it must be sent to a separate entity within the institutional practitioner that enters permissions for logical access controls into the application. The institutional practitioner must authorize at least two individuals or a role filled by at least two individuals to enter the logical access control data. One individual in the separate entity must authenticate to the application and enter the data to grant permissions to individual practitioners to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions. A second individual must authenticate to the application to execute the logical access controls.

(c) The institutional practitioner must retain a record of the individuals or roles that are authorized to conduct identity proofing and logical access control data entry and execution.

(d) Permission to indicate that controlled substances prescriptions are ready to be signed and to sign controlled substance prescriptions must be revoked whenever any of the following occurs, on the date the occurrence is discovered:

(1) An individual practitioner's hard token or any other authentication factor required by the practitioner's two-factor authentication protocol is lost, stolen, or

compromised. Such access must be terminated immediately upon receiving notification from the individual practitioner.

(2) The institutional practitioner's or, where applicable, individual practitioner's DEA registration expires, unless the registration has been renewed.

(3) The institutional practitioner's or, where applicable, individual practitioner's DEA registration is terminated, revoked, or suspended.

(4) An individual practitioner is no longer authorized to use the institutional practitioner's electronic prescription application (e.g., when the individual practitioner is no longer associated with the institutional practitioner.)

§ 1311.135 Requirements for creating a controlled substance prescription.

(a) The electronic prescription application may allow the registrant or his agent to enter data for a controlled substance prescription, provided that only the registrant may sign the prescription in accordance with §§ 1311.120(b)(11) and 1311.140.

(b) If a practitioner holds multiple DEA registrations, the practitioner or his agent must select the appropriate registration number for the prescription being issued in accordance with the requirements of § 1301.12 of this chapter.

(c) If required by State law, a supervisor's name and DEA number may be listed on a prescription, provided the prescription clearly indicates who is the supervisor and who is the prescribing practitioner.

§ 1311.140 Requirements for signing a controlled substance prescription.

(a) For a practitioner to sign an electronic prescription for a controlled substance the following must occur:

(1) The practitioner must access a list of one or more controlled substance prescriptions for a single patient. The list must display the information required by § 1311.120(b)(9).

(2) The practitioner must indicate the prescriptions that are ready to be signed.

(3) While the prescription information required in § 1311.120(b)(9) is displayed, the following statement or its substantial equivalent is displayed: "By completing the two-factor authentication protocol at this time, you are legally signing the prescription(s) and authorizing the transmission of the above information to the pharmacy for dispensing. The two-factor authentication protocol may only be completed by the practitioner whose name and DEA registration number appear above."

(4) While the prescription information required in § 1311.120(b)(9) and the statement required by paragraph (a)(3) of this section remain displayed, the practitioner must be prompted to complete the two-factor authentication protocol.

(5) The completion by the practitioner of the two-factor authentication protocol in the manner provided in paragraph (a)(4) of this section will constitute the signing of the prescription by the practitioner for purposes of § 1306.05(a) and (e) of this chapter.

(6) Except as provided under § 1311.145, the practitioner's completion of the two-factor authentication protocol must cause the application to digitally sign and electronically archive the information required under part 1306 of this chapter.

(b) The electronic prescription application must clearly label as the signing function the function that prompts the practitioner to execute the two-factor authentication protocol using his credential.

(c) Any prescription not signed in the manner required by this section shall not be transmitted.

§ 1311.145 Digitally signing the prescription with the individual practitioner's private key.

(a) An individual practitioner who has obtained a digital certificate as provided in § 1311.105 may digitally sign a controlled substance prescription using the private key associated with his digital certificate.

(b) The electronic prescription application must require the individual practitioner to complete a two-factor authentication protocol as specified in § 1311.140(a)(4) to use his private key.

(c) The electronic prescription application must digitally sign at least all information required under part 1306 of this chapter.

(d) The electronic prescription application must electronically archive the digitally signed record.

(e) A prescription that is digitally signed with a practitioner's private key may be transmitted to a pharmacy without the digital signature.

(f) If the electronic prescription is transmitted without the digital signature, the electronic prescription application must check the certificate revocation list of the certification authority that issued the practitioner's digital certificate. If the digital certificate is not valid, the electronic prescription application must not transmit the prescription. The certificate revocation list may be cached until the certification authority issues a new certificate revocation list.

(g) When the individual practitioner digitally signs a controlled substance prescription with the private key associated with his own digital certificate obtained as provided under § 1311.105, the electronic prescription application is not required to digitally sign the prescription using the application's private key.

§ 1311.150 Additional requirements for internal application audits.

(a) The application provider must establish and implement a list of auditable events. Auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the electronic prescription application, or successful unauthorized access where the determination of such is feasible.

(2) Attempted unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the prescription application.

(4) Any setting of or change to logical access controls related to the issuance of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful creation, modification, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The electronic prescription application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) Any person designated to set logical access controls under §§ 1311.125 or 1311.130 must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the electronic prescription application provider and the Administration within one business day.

§ 1311.170 Transmission requirements.

(a) The electronic prescription application must transmit the electronic prescription as soon as possible after signature by the practitioner.

(b) The electronic prescription application may print a prescription that has been transmitted only if an intermediary or the designated pharmacy notifies a practitioner that an electronic prescription was not successfully delivered to the designated pharmacy. If this occurs, the electronic prescription application may print the prescription for the practitioner's manual signature. The printed prescription must include information noting that the prescription was originally transmitted electronically to [name of the specific pharmacy] on [date/time] and that transmission failed.

(c) The electronic prescription application may print copies of the transmitted prescription if they are clearly labeled: "Copy only - not valid for dispensing." Data on the prescription may be electronically transferred to medical records, and a list of prescriptions written may be printed for patients if the list indicates that it is for informational purposes only and not for dispensing.

(d) The electronic prescription application must not allow the transmission of an electronic prescription if an original prescription was printed prior to attempted transmission.

(e) The contents of the prescription required by part 1306 of this chapter must not be altered during transmission between the practitioner and pharmacy. Any change to the content during transmission, including truncation or removal of data, will render the electronic prescription invalid. The electronic prescription data may be converted from one software version to another between the electronic prescription application and the pharmacy application; conversion includes altering the structure of fields or machine language so that the receiving pharmacy application can read the prescription and import the data.

(f) An electronic prescription must be transmitted from the practitioner to the pharmacy in its electronic form. At no time may an intermediary convert an electronic prescription to another form (e.g., facsimile) for transmission.

§ 1311.200 Pharmacy responsibilities.

(a) Before initially using a pharmacy application to process controlled substance prescriptions, the pharmacy must determine that the third-party auditor or certification organization has found that the pharmacy application does the following accurately and consistently:

(1) Import, store, and display the information required for prescriptions under § 1306.05(a) of this chapter.

(2) Import, store, and display the indication of signing as required by § 1311.120(b)(17).

(3) Import, store, and display the number of refills as required by § 1306.22 of this chapter.

(4) Import, store, and verify the practitioner's digital signature, as provided in § 1311.210(c), where applicable.

(b) If the third-party auditor or certification organization has found that a pharmacy application does not accurately and consistently import, store, and display other information required for prescriptions under this chapter, the pharmacy must not process electronic prescriptions for controlled substances that are subject to the additional information requirements.

(c) If a pharmacy application provider notifies a pharmacy that a third-party audit or certification report indicates that the application or the application provider no longer meets the requirements of this part or notifies it that the application provider has identified an issue that makes the application non-compliant, the pharmacy must immediately cease to process controlled substance prescriptions using the application.

(d) A pharmacy that receives a notification that the pharmacy application is not in compliance with the requirements of this part must not use the application to process controlled substance prescriptions until it is notified that the application is again compliant and all relevant updates to the application have been installed.

(e) The pharmacy must determine which employees are authorized to enter information regarding the dispensing of controlled substance prescriptions and annotate or alter records of these prescriptions (to the extent such alterations are permitted under this chapter). The pharmacy must ensure that logical access controls in the pharmacy

application are set so that only such employees are granted access to perform these functions.

(f) When a pharmacist fills a prescription in a manner that would require, under part 1306 of this chapter, the pharmacist to make a notation on the prescription if the prescription were a paper prescription, the pharmacist must make the same notation electronically when filling an electronic prescription and retain the annotation electronically in the prescription record or in linked files. When a prescription is received electronically, the prescription and all required annotations must be retained electronically.

(g) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to the pharmacy, the pharmacist must check its records to ensure that the electronic version was not received and the prescription dispensed. If both prescriptions were received, the pharmacist must mark one as void.

(h) When a pharmacist receives a paper or oral prescription that indicates that it was originally transmitted electronically to another pharmacy, the pharmacist must check with that pharmacy to determine whether the prescription was received and dispensed. If the pharmacy that received the original electronic prescription had not dispensed the prescription, that pharmacy must mark the electronic version as void or canceled. If the pharmacy that received the original electronic prescription dispensed the prescription, the pharmacy with the paper version must not dispense the paper prescription and must mark the prescription as void.

(i) Nothing in this part relieves a pharmacy and pharmacist of the responsibility to dispense controlled substances only pursuant to a prescription issued for a legitimate medical purpose by a practitioner acting in the usual course of professional practice.

§ 1311.205 Pharmacy application requirements.

(a) The pharmacy may only use a pharmacy application that meets the requirements in paragraph (b) of this section to process electronic controlled substance prescriptions.

(b) The pharmacy application must meet the following requirements:

(1) The pharmacy application must be capable of setting logical access controls to limit access for the following functions:

(i) Annotation, alteration, or deletion of prescription information.

(ii) Setting and changing the logical access controls.

(2) Logical access controls must be set by individual user name or role.

(3) The pharmacy application must digitally sign and archive a prescription on receipt or be capable of receiving and archiving a digitally signed record.

(4) For pharmacy applications that digitally sign prescription records upon receipt, the digital signature functionality must meet the following requirements:

(i) The cryptographic module used to digitally sign the data elements required by part 1306 of this chapter must be at least FIPS 140-2 Security Level 1 validated. FIPS 140-2 is incorporated by reference in § 1311.08.

(ii) The digital signature application and hash function must comply with FIPS 186-3 and FIPS 180-3, as incorporated by reference in § 1311.08.

(iii) The pharmacy application's private key must be stored encrypted on a FIPS 140-2 Security Level 1 or higher validated cryptographic module using a FIPS-approved encryption algorithm. FIPS 140-2 is incorporated by reference in § 1311.08.

(iv) For software implementations, when the signing module is deactivated, the pharmacy application must clear the plain text password from the application memory to prevent the unauthorized access to, or use of, the private key.

(v) The pharmacy application must have a time application that is within five minutes of the official National Institute of Standards and Technology time source.

(5) The pharmacy application must verify a practitioner's digital signature (if the pharmacy application accepts prescriptions that were digitally signed with an individual practitioner's private key and transmitted with the digital signature).

(6) If the prescription received by the pharmacy application has not been digitally signed by the practitioner and transmitted with the digital signature, the pharmacy application must either:

(i) Verify that the practitioner signed the prescription by checking the data field that indicates the prescription was signed; or

(ii) Display the field for the pharmacist's verification.

(7) The pharmacy application must read and retain the full DEA number including the specific internal code number assigned to individual practitioners authorized to prescribe controlled substances by the hospital or other institution as provided in § 1301.22(c) of this chapter.

(8) The pharmacy application must read and store, and be capable of displaying, all information required by part 1306 of this chapter.

(9) The pharmacy application must read and store in full the information required under § 1306.05(a) of this chapter. The pharmacy application must either verify that such information is present or must display the information for the pharmacist's verification.

(10) The pharmacy application must provide for the following information to be added or linked to each electronic controlled substance prescription record for each dispensing:

(i) Number of units or volume of drug dispensed.

(ii) Date dispensed.

(iii) Name or initials of the person who dispensed the prescription.

(11) The pharmacy application must be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name, and date dispensed.

(12) The pharmacy application must allow downloading of prescription data into a database or spreadsheet that is readable and sortable.

(13) The pharmacy application must maintain an audit trail of all actions related to the following:

(i) The receipt, annotation, alteration, or deletion of a controlled substance prescription.

(ii) Any setting or changing of logical access control permissions related to the dispensing of controlled substance prescriptions.

(iii) Auditable events as specified in § 1311.215.

(14) The pharmacy application must record within each audit record the following information:

(i) The date and time of the event.

(ii) The type of event.

(iii) The identity of the person taking the action, where applicable.

(iv) The outcome of the event (success or failure).

(15) The pharmacy application must conduct internal audits and generate reports on any of the events specified in § 1311.215 in a format that is readable by the pharmacist. Such an internal audit may be automated and need not require human intervention to be conducted.

(16) The pharmacy application must protect the stored audit records from unauthorized deletion. The pharmacy application shall prevent modifications to the audit records.

(17) The pharmacy application must back up the controlled substance prescription records daily.

(18) The pharmacy application must retain all archived records electronically for at least two years from the date of their receipt or creation and comply with all other requirements of § 1311.305.

§ 1311.210 Archiving the initial record.

(a) Except as provided in paragraph (c) of this section, a copy of each electronic controlled substance prescription record that a pharmacy receives must be digitally signed by one of the following:

(1) The last intermediary transmitting the record to the pharmacy must digitally sign the prescription immediately prior to transmission to the pharmacy.

(2) The first pharmacy application that receives the electronic prescription must digitally sign the prescription immediately on receipt.

(b) If the last intermediary digitally signs the record, it must forward the digitally signed copy to the pharmacy.

(c) If a pharmacy receives a digitally signed prescription that includes the individual practitioner's digital signature, the pharmacy application must do the following:

(1) Verify the digital signature as provided in FIPS 186-3, as incorporated by reference in § 1311.08.

(2) Check the validity of the certificate holder's digital certificate by checking the certificate revocation list. The pharmacy may cache the CRL until it expires.

(3) Archive the digitally signed record. The pharmacy record must retain an indication that the prescription was verified upon receipt. No additional digital signature is required.

§ 1311.215 Internal audit trail.

(a) The pharmacy application provider must establish and implement a list of auditable events. The auditable events must, at a minimum, include the following:

(1) Attempted unauthorized access to the pharmacy application, or successful unauthorized access to the pharmacy application where the determination of such is feasible.

(2) Attempted or successful unauthorized modification or destruction of any information or records required by this part, or successful unauthorized modification or destruction of any information or records required by this part where the determination of such is feasible.

(3) Interference with application operations of the pharmacy application.

(4) Any setting of or change to logical access controls related to the dispensing of controlled substance prescriptions.

(5) Attempted or successful interference with audit trail functions.

(6) For application service providers, attempted or successful annotation, alteration, or destruction of controlled substance prescriptions or logical access controls related to controlled substance prescriptions by any agent or employee of the application service provider.

(b) The pharmacy application must analyze the audit trail at least once every calendar day and generate an incident report that identifies each auditable event.

(c) The pharmacy must determine whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records. Any such incidents must be reported to the pharmacy application service provider, if applicable, and the Administration within one business day.

§ 1311.300 Application provider requirements - Third-party audits or certifications.

(a) Except as provided in paragraph (e) of this section, the application provider of an electronic prescription application or a pharmacy application must have a third-party audit of the application that determines that the application meets the requirements of this part at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.

(2) Whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first.

(b) The third-party audit must be conducted by one of the following:

(1) A person qualified to conduct a SysTrust, WebTrust, or SAS 70 audit.

(2) A Certified Information System Auditor who performs compliance audits as a regular ongoing business activity.

(c) An audit for installed applications must address processing integrity and determine that the application meets the requirements of this part.

(d) An audit for application service providers must address processing integrity and physical security and determine that the application meets the requirements of this part.

(e) If a certifying organization whose certification process has been approved by DEA verifies and certifies that an electronic prescription or pharmacy application meets the requirements of this part, certification by that organization may be used as an alternative to the audit requirements of paragraphs (b) through (d) of this section, provided that the certification that determines that the application meets the requirements of this part occurs at each of the following times:

(1) Before the application may be used to create, sign, transmit, or process controlled substance prescriptions.

(2) Whenever a functionality related to controlled substance prescription requirements is altered or every two years, whichever occurs first.

(f) The application provider must make the audit or certification report available to any practitioner or pharmacy that uses the application or is considering use of the

application. The electronic prescription or pharmacy application provider must retain the most recent audit or certification results and retain the results of any other audits or certifications of the application completed within the previous two years.

(g) Except as provided in paragraphs (h) and (i) of this section, if the third-party auditor or certification organization finds that the application does not meet one or more of the requirements of this part, the application must not be used to create, sign, transmit, or process electronic controlled substance prescriptions. The application provider must notify registrants within five business days of the issuance of the audit or certification report that they should not use the application for controlled substance prescriptions. The application provider must also notify the Administration of the adverse audit or certification report and provide the report to the Administration within one business day of issuance.

(h) For electronic prescription applications, the third-party auditor or certification organization must make the following determinations:

(1) If the information required in § 1306.05(a) of this chapter, the indication that the prescription was signed as required by § 1311.120(b)(17) or the digital signature created by the practitioner's private key, if transmitted, and the number of refills as required by § 1306.22 of this chapter, cannot be consistently and accurately recorded, stored, and transmitted, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part.

(2) If other information required under this chapter cannot be consistently and accurately recorded, stored, and transmitted, the third-party auditor or certification organization must indicate that the application has failed to meet the requirements for the

specific information and should not be used to create, sign, and transmit prescriptions that require the additional information.

(i) For pharmacy applications, the third-party auditor or certification organization must make the following determinations:

(1) If the information required in § 1306.05(a) of this chapter, the indication that the prescription was signed as required by § 1311.205(b)(6), and the number of refills as required by § 1306.22 of this chapter, cannot be consistently and accurately imported, stored, and displayed, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part.

(2) If the pharmacy application accepts prescriptions with the practitioner's digital signature, the third-party auditor or certification organization must indicate that the application does not meet the requirements of this part if the application does not consistently and accurately import, store, and verify the digital signature.

(3) If other information required under this chapter cannot be consistently and accurately imported, stored, and displayed, the third-party auditor or certification organization must indicate that the application has failed to meet the requirements for the specific information and should not be used to process electronic prescriptions that require the additional information.

§ 1311.302 Additional application provider requirements.

(a) If an application provider identifies or is made aware of any issue with its application that make the application non-compliant with the requirements of this part, the application provider must notify practitioners or pharmacies that use the application as soon as feasible, but no later than five business days after discovery, that the application should not be used to issue or process electronic controlled substance prescriptions.

(b) When providing practitioners or pharmacies with updates to any issue that makes the application non-compliant with the requirements of this part, the application provider must indicate that the updates must be installed before the practitioner or pharmacy may use the application to issue or process electronic controlled substance prescriptions.

§ 1311.305 Recordkeeping.

(a) If a prescription is created, signed, transmitted, and received electronically, all records related to that prescription must be retained electronically.

(b) Records required by this subpart must be maintained electronically for two years from the date of their creation or receipt. This record retention requirement shall not pre-empt any longer period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to practitioners, pharmacists, or pharmacies.

(c) Records regarding controlled substances prescriptions must be readily retrievable from all other records. Electronic records must be easily readable or easily rendered into a format that a person can read.

(d) Records required by this part must be made available to the Administration upon request.

(e) If an application service provider ceases to provide an electronic prescription application or an electronic pharmacy application or if a registrant ceases to use an application service provider, the application service provider must transfer any records subject to this part to the registrant in a format that the registrant's applications are capable of retrieving, displaying, and printing in a readable format.

(f) If a registrant changes application providers, the registrant must ensure that any records subject to this part are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

(g) If a registrant transfers its electronic prescription files to another registrant, both registrants must ensure that the records are migrated to the new application or are stored in a format that can be retrieved, displayed, and printed in a readable format.

(h) Digitally signed prescription records must be transferred or migrated with the digital signature.

_ Dated: March 22, 2010

Michele M. Leonhart,
Deputy Administrator.

[FR Doc. 2010-6687 Filed 03/24/2010 at 4:15 pm; Publication Date: 03/31/2010]